The Security Times

SPECIAL EDITION OF THE ATLANTIC TIMES FOR THE 5TH MSC CORE GROUP MEETING

November 2013 — Berlin, Germany

In this issue

NSA Merkel affair pages 4-7

Cyber security pages 21-28

Call of duty

Germany must "Europeanize" its activities in foreign and security policy

By Wolfgang Ischinger

FOTOLIA/CLAUDIA PEREZ LEAL/TM

Fortunately, the worries that some of our neighbors had some 20 years ago, namely that Germany may have to be feared again, have not come true. And yet, as Timothy Garton Ash said at the Munich Security Conference in 2012, we have "a European Germany in a German Europe."

This European Germany is today, without a doubt, the central economic power in Europe. However, in terms of security policy, Germany does not play an active and formative role commensurate to our size and potential. Our partners' expectations of us are not exaggerated – and criticism that Germany sometimes gladly shies away from the action, particularly when things get difficult, does not always seem entirely unfounded.

We Germans have lived quite comfortably with the status quo. We do not want change. We would prefer to be left alone to enjoy our growing prosperity. It was not always like that. Before reunification – as was set out in the German Basic Law – the old Federal Republic of Germany was an "anti-status quo" power: we had the objective of overcoming the division of Germany and Europe.

Since reunification, attitudes have changed. We would have liked to freeze the course of history. But the belief that we could isolate ourselves from the world's problems, rather like a Switzerland writ large, is a fatal misconception. The wheels of change are turning around us in a spectacular way, and we are called upon not only to face this challenge, but also to actively embrace it.

The "rise of the rest," – of countries like China, Brazil, and India – means that the world order is becoming less clear-cut and international actions and decisions are becoming more complex and complicated. The relative influence of Germany and Europe (and the West as a whole) will decrease; by 2050, Europe will make up no more than about 7 percent of the world's population.

In the future, the US will devote more attention and resources to eastern Asia and be less involved with Europe and its neighboring countries. This does not mean that the US will "abandon" Europe. However, Europe will need to become more independent in terms of security policy. We do not yet seem to have understood what this means for us.

And whether we like it or not, Germany has become the key country of the EU. For the foreseeable future, Germany will remain Europe's "indispensable nation," as Polish foreign minister Radek Sikorski put it in his historic speech in the fall of 2011 in Berlin. The creative drive coming from Berlin, or the lack thereof, will be a decisive factor for whether and how Europe is made viable for the future.

> "Does anyone seriously want to claim, in the face of the monumental global changes, that we Germans can achieve anything on our own?"

Fundamentally, this means two things. First, we must "Europeanize" our activities in foreign and security policy much more. There is no longer any workable alternative to further integration and more joint action. Does anyone seriously want to claim, in the face of the monumental global changes, that we Germans can achieve anything on our own? Paul-Henri Spaak's famous words are even more true today than in the past: "There are only two types of states in Europe: small states, and small states that have not yet realized that they are small."

Second, we Germans must not be afraid to take on joint leadership responsibility. This does not mean that we should act as Europe's hegemon, or even indulge in arrogant flights of fancy. It means, however, that we should learn and practice "generous leadership" – because this is in our fundamental best interest. However, leadership – broad-minded leadership – is never entirely free of charge.

In the coming months we will have to put our cards on the table about the type of Europe we want. Up to now, for tactical reasons, mainly specific issues such as bailout packages and banking unions have been on the agenda. However, the big questions can no longer be avoided if we want to develop the EU further and keep the euro afloat. A stronger Europe is only possible with a strengthening of the European institutions, in particular the European Parliament and the Commission. The basic principle should be: find intergovernmental solutions only as often as required; strengthen European institutions as significantly as possible.

The new German government and the French government now have a window of over three years before their next elections. The current Polish government, for instance, would offer strong partnership in identifying the path to a stronger EU and to a political union.

Wolfgang Ischinger, Germany's former ambassador to the US and the UK, is the Chairman of the Munich Security Conference since 2008.

MSC

Europe

A key area in which significant progress in integration is necessary and possible in Europe is security and defense policy. In December, the European Council will, for the first time in years, deal primarily with questions of security and defense.

The necessity of finally bringing the concept of integration to bear on security and defense policy is clear: It is scandalous how little bang for the buck we get in Europe. The defense expenditure of all the European countries together totals just under 40 percent of US defense expenditure – and actual military power is only a small fraction of that of the US. At the same time, the EU countries have six times as many different weapons systems as the US. In view of the high fixed costs of armaments, this fragmentation is irresponsible.

A study conducted by McKinsey in conjunction with the Munich Security Conference calculated that European countries could save up to 30 percent per year – that is €13 billion annually – if they worked more closely together in their weapons procurement.

Continued on page 8

Is Europe losing its geopolitical relevance?

Aggregating foreign and defense policy, not renationalization is the way forward

By Charles A. Kupchan

With the EU still struggling to reclaim lasting financial stability and restore economic growth, European elites and publics alike remain preoccupied with issues of debt, bailouts, and jobs. This focus on economic issues is as it should be; the Eurozone crisis, which is not yet definitively over, has the potential to bring down the European Union.

Nonetheless, this focus on the economy is distracting attention from another issue in need of urgent attention: the worsening condition of European defense capabilities.

The Eurozone crisis is taking a serious toll on the EU's aspirations to become a more capable actor on security issues. Austerity has contributed to steady declines in defense spending. Since 2008, defense expenditure among EU members has declined by some 10 percent. Most EU members fail to meet the NATO benchmark of spending at least 2 percent of GDP on defense.

Of even greater negative impact on the prospects for European progress on defense has been the political renationalization spawned by the financial crisis. The fabric of European solidarity has badly frayed as national publics angrily pull away from Brussels and from each other. According to a recent Pew poll, "positive views of the European Union are at or near their low point in most EU nations, even among the young, the hope for the EU's future."

The renationalization of European politics has the potential to snuff out the EU's geopolitical ambitions. Even if they were to increase their defense expenditures, individual European countries are not large enough to play on the global stage. Europe can be an effective security actor only if EU member states aggregate their will and capability. More defense spending would help, but pooling and specialization are essential to establishing a credible European defense capability.

EU members have long been reluctant to deepen collective governance on foreign and defense policy; national security has always been the last redoubt of sovereignty.

The current renationalization of European politics is only making matters worse. It is indeed a cruel irony that the Lisbon Treaty created the foreign policy institutions needed to give the EU more international heft just as the political solidarity needed to backstop those institutions began to fray.

Political developments among the EU's larger members are particularly troubling. Germany, perhaps as a reaction against the involvement of its troops in Afghanistan, is turning inward. Berlin's decision to abstain on the UN vote authorizing military action in Libya was a clear indicator. So was a recent federal election campaign in which the candidates behaved as if all issues beyond German borders were irrelevant. On matters of geopolitics, Germany is increasingly missing in action.

Meanwhile, Britain has been busily slashing its defense spending and distancing itself from the EU. Faced with anti-EU sentiment among Conservatives and the growing political strength of the UK Independence Party, which calls for Britain to quit the EU, Prime Minister David Cameron is seeking to loosen London's ties to Brussels. As a consequence either of London's continuing drift from the continent or of a referendum on EU membership that potentially looms on the horizon, Britain could well leave the EU within a few years. Even if it stays put, London will certainly not be leading the charge to pool sovereignty on matters of foreign and security policy.

The French are the last men standing. Paris has the will and capability to be a European leader on defense. It pushed for and was a major contributor to NATO's military operation in Libya, intervened unilaterally in Mali, and was prepared to join the United States in a military response to the Syrian regime's use of chemical weapons. The French, however, have jealously guarded their national prerogatives on defense, and prefer an European Union of strong states, not one of strong supranational governance. At least for now, the push to collectivize European defense will not be coming from Paris.

The timing of Europe's backsliding on defense is not good. The EU's efforts to raise its geopolitical profile are running out of steam just as its American partner is also turning inward. War weariness, budget constraints, and domestic polarization are taking a heavy toll on America's readiness to be the global guardian of last resort. As US President Barack Obama repeatedly proclaimed during his bid for reelection, "It is time for nation-building here at home." With the US in retrenchment mode, there is a pressing need for the EU to help fill the resulting gap. At least for now, that will not happen.

Transatlantic ties are poised to suffer accordingly. Washington will be less likely to invest in NATO if Europe grows incapable of being a credible partner. The United States has long complained about transatlantic burden-sharing. But the US pivot to Asia, the budget sequester, and the turning inward among both Democrats and Republicans endows the issue with unprecedented salience. As the former US Secretary of Defense Robert Gates stated in 2011, NATO's future will be "dim, if not dismal," should Europeans continue to underfund defense. "Future US political leaders," Gates warned, "may not consider the return on America's investment in NATO worth the cost."

A weak and introverted Europe also spells trouble for the broader task of managing a global landscape in the midst of profound change. For the first time since World War II, the output of the advanced industrialized democracies represents less than 50 percent of global GDP. The aggregate GDP of China is expected to surpass that of the United States within roughly 15 years. Asia already outspends Europe on defense. A major change in the global pecking order is afoot.

Not only is the West's material primacy waning, but its norms and values are also under threat. The Arab Awakening has done more to fuel political Islam than liberal democracy. State capitalism is alive and well in Russia and China. Even emerging democracies like India and Brazil question key Western preferences, such as the penchant for promoting democracy and the enforcement of the Responsibility to Protect.

Under these circumstances, the United States and Europe need to show renewed solidarity in defense of a liberal international order. That task is likely to go unfulfilled if both the United States and the EU are preoccupied by internal challenges and allow their security partnership to atrophy.

There is one ray of light on the horizon. In their struggle to end the Eurozone crisis, member states envisage a deeper economic union – one capable of giving Europe the banking and financial oversight it needs to function effectively as a currency union. Admittedly, the process of deepening is occurring slowly, with Germany reluctant to move toward a banking union and the collectivization of debt until member states have carried out further reforms.

PRIVATE

Charles A. Kupchan is a professor of international affairs at Georgetown University and a senior fellow at the Council on Foreign Relations and the Transatlantic Academy.

Europe

However, if and when that tighter economic union takes shape, it is possible that the push for deeper integration will spill over into the security realm. If national publics and governments come to see the value of collective governance on economic issues, they may then be more ready to accept a deeper union on matters of foreign and security policy. Put differently, if European unity is able to deliver the goods on the economic front, then publics are more likely to place confidence in the union's ability to deliver on the security front as well.

For now, regrettably, the most likely outcome is a Europe that gradually loses its geopolitical relevance. That outcome would be a severe setback not only for Europe, but also for a world much in need of European engagement and values. Perhaps that prospect alone will reawaken Europeans and encourage them to band together in the service of global responsibility. ■

Increasing risk of floundering

Does Europe have a future as a strategic actor ?

By François Heisbourg

During the fifteen years that followed the fall of the Berlin Wall, Europe as a whole began to emerge as a strategic actor in its own right. The European Community, which became the European Union in 1993, greatly extended its sphere of competence. Beyond the completion of the single market, the EU embarked on the creation of a single currency, put in place the Schengen border agreements along with growing convergence in judicial and home affairs and began to embark on a common foreign and security policy, which from 1999 onwards also included a military dimension.

A convention, so named after the body that framed the constitution of the newly independent United States of America, was busy drafting a constitutional treaty for the European Union. At the same time, the EU was developing as a 'normative empire' across a broad spectrum of international endeavors, from trade regulation or technological innovation to the Kyoto protocol on climate change, while playing a lead role in the framing of major initiatives such as the International Criminal Court or the Responsibility-to-Protect.

In directly strategic terms, the EU's enlargement from a grouping of nine members at the end of the Cold War to a continent-wide club of 28 states was a remarkable and historically unprecedented case of entirely voluntary and peaceful empire-building on an epic scale. While the US – through NATO – provided the security umbrella, the EU with its *acquis communautaire* was the prime mover in transforming the societies of the erstwhile Soviet Empire into fully fledged members of the democratic family of European and Atlantic nations.

Overall, this was an impressive set of achievements. But it was also an incomplete process, putting the Europeans right in the middle of the stream, to borrow a metaphor from former German Foreign Minister Joschka Fischer. That is not a place where one can stay: you either swim forward (to an ever more federal outcome) or backward (and recover to eventually begin anew: but this the Union has never done) – or you sink.

Unfortunately, Europe got caught midstream nearly ten years ago and is at increasing risk of floundering. First, with the deep divisions caused by the US-British invasion of Iraq in 2003, came the limitation of the ambitions of Europe's Security and Defense Policy (ESDP). With UK forces and British political will largely unavailable for ESDP's operations and further development, the Union's military persona has remained embryonic.

Then, in 2005, came the double shock of the rejection of the constitutional treaty by France and the Netherlands, two of the six founding members of the Union. Within three years, the Europeans were sucked into the vortex of the global financial crisis, which left policymakers with little time or energy for moving forward on other issues. The ratification of the Lisbon treaty in late 2009 was one last heave before putting on hold any initiatives not related to the management of the economic, financial and monetary situation.

To make matters worse, not only is the EU stuck in mid-stream, but the waters are becoming more turbulent. First, the member states have less money available for defense and foreign affairs, with defense spending dropping by some 15 percent on average since the crisis began. Although common sense as well as plentiful and well-meaning political statements suggest that as a consequence the Europeans should pool and share defense assets, the reality looks slightly different.

When deep disagreements occur, such as over the war in Libya, can all partners rely on the immediate availability of pooled and shared assets? And has anyone yet met a national politician who is ready to say: 'Yes of course, I will agree to close the tank/plan factory or naval shipyard in my constituency, since the neighboring country produces cheaper and better tanks/planes/ships than we do'?

There is a fair amount of low-hanging fruit available in terms of pooling and sharing in training, maintenance, testing, logistics, and certification activities and the like. But it will not make up for the continuing reduction in our overall defense efforts.

In the meantime, the United States is facing China's rise and the reduction of its own defense spending. Its energy revolution is reducing its dependence on the Middle East. This is also a country that has witnessed two consecutive strategic failures in Iraq and Afghanistan: the US population is not looking for new monsters to slay.

Within NATO, the US will act as a more reluctant partner, as we saw in NATO's Libya campaign, and again in NATO's recent "Steadfast Jazz" exercise in Poland and the Baltics (in which the Americans, like the Germans, were mostly absent). At the same time, the US military-industrial complex, heavily challenged by domestic budget cuts, will expect the NATO Europeans to buy American in the name of Smart Defense. Tough (or tougher) love will be America's overall attitude towards a Europe otherwise left to its own devices.

Europe's security environment is deteriorating precisely at the moment when its collective will and capabilities are diminishing, with a more reticent US and a more instrumental NATO. The Arab revolutions are not only turning ugly in most instances – Syria, Libya, Egypt – and new ones may well break out in areas either close to Europe (notably post-Bouteflika Algeria, possibly Morocco) or critical to its interests, such as in Saudi Arabia, with no clear line of succession and a frustrated, bored and largely unemployed youth population. Nor is the situation in the Sahel any more encouraging. The human tragedies of Lampedusa, Ceuta and Melilla show what may be in store for a Europe unable to think and act collectively in the face of challenges that are its own, not those of the US or Asia.

Finally, we will have to contend with a Russia which is both able to act assertively and unable to modernize its quasi-Arabian petro-economy and its Algerian-style power vertical. Precisely because the EU exercises immense attraction to the countries on Russia's periphery, notably Ukraine, we must also expect more energetic pushing back by Russia.

So what are the possible scenarios for an EU stuck in the middle of the roiling waters of international life, not to mention domestic turbulences as the temptation of populism rises?

The most optimistic and rather unlikely scenario involves the combination of a return to substantial growth in most of the Eurozone countries, defusing the rise of extremism, while a set of robust federal measures make the Euro sustainable in the long run. These involve the creation of a true, US-style, banking union (not the supervisory mechanism currently being considered), a large federal budget, substantial portability of social security regimes: in effect, the sorts of things which allow Brazil, India, the US or Switzerland to each sustain a common currency. Given the state of public opinion in most EU/Eurozone countries, the chances of this happening in a politically transparent way are low. Last but not least, that Britain does not leave the EU under such circumstances.

A variation of the above is much more likely. A limited degree of federalization is put in place with an element of stealth, much as has happened for the creation of new institutions and practices related to the Euro's rescue, enough to save the Euro (at least until a major new shock overwhelms it in a decade or two). But given the state of British public opinion, such measures could be enough to prompt the UK's exit.

In economic terms, this may be dealt with, but from a strategic standpoint the consequences could be quite unfortunate. With Britain drifting towards the Atlantic, the 'rump EU' would be centered on Germany in political and strategic terms, much as the Eurozone already is from an economic and financial standpoint.

In today's Eurozone, Germany's prudence, along with the fairly narrowly defined spectrum of issues covered, the hegemony question has proven to be manageable, with Germanophobia remaining a limited problem. Once transformed into a Continental System, to use Napoléon's words, divided by the divergent strategic cultures of Germany and France, the EU would find it even more difficult than today to emerge as a coherent strategic actor.

Yet another possibility is one in which the Euro explodes catastrophically. Although thanks to Mario Draghi, the President of the European Central Bank, this no longer appears to be a scenario of immediate concern, it cannot be excluded. Under such cataclysmic conditions, the EU may well disappear as well, given the immense store of bad will which would result from a disorderly breakup of the euro. The strategic consequences could be quite lurid, although it is unlikely that world war could be a consequence in the absence of a credible candidate for Napoleonic, Wilhelminian or Hitlerite hegemony in a declining and aging Europe.

Finally, there is the theoretical scenario of an orderly unraveling of the Euro, which would restore the EU to its situation of the mid-1990s: in effect returning us to the river bank from which we came. Although I have argued that such an achievement is economically doable and strategically desirable, the political investment made by our countries and their leaders in the Euro is such that probably none will summon the will to suggest collectively ending an experiment which has failed in its intent to generate growth and foster greater political union. ■

PRIVATE

François Heisbourg, is a special adviser at the Foundation for Strategic Research in Paris.

Europe

Sharing is caring

EU leaders to resume talks on Common Security and Defense Policy

In March 2011, French and British forces intervened in Libya's civil war, implementing a no-fly zone and enforcing an arms embargo to protect civilians. The US backed the operation, which was actively supported by a number of European states. But others, including Germany and Poland, rejected military action. The NATO-led operation was called "Unified Protector" – but it revealed a lack of unity. It revealed that Europe has no common security and defense policy (CSDP) worth the name.

The goal of CSDP, with which Europe would both guarantee its own security and take on more global responsibility, was enshrined in the Maastricht Treaties in 1993. The EU has not come far since. In July 2013, the European Commission concluded: "The successive waves of cuts in defense budgets and the persisting fragmentation of defense markets threaten Europe's capacity to sustain effective defense capabilities and a competitive defense industry."

Late last year EU Council President Herman van Rompuy announced his intention to "devote the December 2013 European Council to these questions." The EU heads of state and government will again debate the CSDP and Europe's contribution to global security structures.

Whether the leaders of the EU member states, now 28 in all, each of whom has their own ideas about security policy and state sovereignty, will speak with one voice on questions of defense, foreign, and security policy, is doubtful to say the least. European leaders tend to favor bilateral agreements – see the UK-French Lancaster House treaty for defense and security cooperation. In general, most Europeans do not appear to savor military operations, let alone interventions in faraway conflicts, preferring to leave such matters to the US. Yet Washington is pivoting toward the Asia-Pacific region and would prefer to see Europe solve its own regional problems. Financial strictures are forcing governments practically across the board to cut defense budgets.

At the meeting of EU Foreign and Defense Ministers in Vilnius in September, EU Foreign Policy Chief Catherine Ashton circulated an 18-page report that said the security of Europe has been a historical prerequisite for its economic welfare. "We now need to avoid that Europe's economic difficulties will affect its capacity to maintain its own security," the report said.

Yet the austerity imperative could also enhance willingness to divide up the tasks and readiness to have more defense cooperation instead of holding onto redundant capabilities. Unfortunately, the rhetoric of recent years that has invoked the slogan of "pooling and sharing" has not been followed by any significant action. Defense expenditures within the EU remain very uneven and there is still no agreed long-term vision for CSDP. And, as Ashton pointed out, "decision-making on new operations or missions is often cumbersome and long. And securing Member States' commitment to support missions and operations, especially when it comes to accepting risk and costs, can be challenging, resulting in force generation difficulties."

To be sure, the EU has gained plaudits with operations such as that off the Horn of Africa against piracy. Yet it is still not a reliable "security provider" and building block of global security architecture. In Mali, as in Libya, it was again one European state that intervened militarily while others advocated diplomacy – and not only because of the parliamentary prerogative that 18 EU states have in deciding whether to commit troops to foreign missions.

Obviously, Europe does not speak with one voice in security and defense questions. Perhaps the summit in December will dare to take the first steps to change that. But in what direction? And with what objectives? Catherine Ashton put it this way: "European citizens and the international community need to be able to rely on the EU to deliver when the situation demands." *PHK*

'Our country is not an island'

Federal President Joachim Gauck on Germany's duty in Europe and the world

What is Germany's duty in Europe and in the world? Some neighboring countries fear Germany taking on a strong role, others desire it. Even we ourselves waver – assuming less responsibility is no longer an option and we must now adjust to taking on more responsibility.

Five years after the end of World War II, the political philosopher Hannah Arendt wrote: "It looks as if, having been denied world domination, the Germans have fallen in love with powerlessness."

Germany had reduced Europe to ruins and destroyed millions of human lives. What Arendt described as powerlessness had a political dimension. A defeated Germany had to earn new trust and regain its sovereignty.

On a visit to France a few weeks ago, I was confronted with the question: do we Germans remember our past so actively because we seek an excuse not to deal with the world's contemporary problems and conflicts? Are we letting others foot the bill for our insurance policies?

Of course we have grounds to contradict this view. The Bundeswehr is helping to keep the peace in Afghanistan and Kosovo. Germany is supporting the International Criminal Court, is promoting a global climate agreement and is actively engaged in development cooperation. Germany's contributions and guarantees are helping to stabilize the Eurozone.

Nevertheless both in our country and elsewhere voices calling for more German engagement in international politics are growing louder. The calls come from a Polish foreign minister as well as professors from Oxford and Princeton. They view Germany as a sleepwalking giant or a spectator of global affairs. One of my predecessors, Richard von Weizsäcker, encourages Germany to more strongly advocate a European foreign and security policy. He sees Germany as a role model.

Joachim Gauck.

PAZ/DPA/W. KUMM

This begs the question – is our engagement on a par with the weight that our country carries? Germany is populous, lies at the heart of the continent and is the world's fourth largest economy. The strength of our country lies in the fact that we have made friends of all of our neighbors and become a reliable partner in international alliances. Integrated and accepted as such, Germany was able to secure freedom, peace and prosperity. Maintaining this political and military stability in uncertain times and ensuring its future viability is our most important concern.

Therefore it is right if, along with others, we ask ourselves: Is Germany fully living up to its responsibility with regard to our neighbors in the East, the Middle East and the southern Mediterranean? What is Germany doing to help aspiring emerging countries to become partners on the international stage?

And if we seek a permanent seat on the United Nations Security Council – what role are we prepared to play in crises in far flung regions of the world?

Our country is not an island. We should not cherish the illusion that we will be spared from political and economic, environmental and military conflicts if we do not contribute to solving them.

I do not like the idea that Germany talks itself up to impose its will on others. Yet neither do I like the idea that Germany talks itself down to eschew risks or solidarity. A country that views itself as part of a whole in this way should encounter neither rejection amongst us Germans, nor mistrust among our neighbors. ■

This is an extract from President Joachim Gauck's speech on Oct. 3 at the official ceremony in Stuttgart marking the 23rd Day of German Unity.

Summer of Snowden

The NSA leaks made headlines in Germany long before the Merkel spying allegation

June 6: Glenn Greenwald, writing in The Guardian, exposes the NSA surveillance program, citing documents provided by the former intelligence contractor Edward Snowden. The report alleges mass NSA surveillance of telephone and Internet data in the US and other nations.

June 8: US President Barack Obama says the NSA's surveillance programs strike "the right balance" between security and privacy. The programs were subject to close oversight by US courts and Congress, he said.

June 17: German Minister of the Interior Hans-Peter Friedrich (CSU) says: "Before anyone even knows exactly what the Americans are doing, everyone is getting worked up and complaining about them. I find this combination of anti-Americanism and naivety really irritating."

June 17: The Guardian publishes information derived from the Snowden documents claiming that Britain's Government Communications Headquarters (GCHQ) spied on participants of the G-20 summit in London in 2009.

June 19: "This is not eavesdropping" – President Obama says during a visit to Berlin that the NSA did not listen to telephone conversations and US secret services could "not browse through regular e-mails by German, American or French citizens." Angela Merkel says: "If you're in Germany, you have to abide by German law... Just because something is technically possible, doesn't mean you're allowed to do it."

July 1: German government spokesman Steffen Seibert says "Spying among friends is unacceptable. The Cold War is over." He is reacting to reports that US intelligence services bugged in the European Union's diplomatic mission in Washington and with the UN in New York.

July 12: The German Interior Minister travels to Washington to meet with US officials. He praises the "noble objective" of the US surveillance program, namely "to save lives in Germany."

July 14: In a TV interview Angela Merkel says that she is "not aware of being spied on."

Aug. 12: Following a meeting of the Bundestag's intelligence oversight committee, Merkel's chief of staff Ronald Pofalla dismisses claims of mass NSA surveillance of Germans: "The claim of the alleged total reconnaissance in Germany is off the table. There is no million-fold violation of basic rights in Germany."

Aug. 16: Returning from his trip to Washington, German Interior Minister Friedrich says that "all the allegations that were raised, have been cleared up."

Oct. 24: German news weekly Der Spiegel reports that an investigation by German intelligence, prompted by research from the magazine, found plausible information that Merkel's cellphone was targeted by a US intelligence agency. Merkel calls the White House to demand clarification. ■

The Security Times

Publisher: Detlef W. Prinz
Executive Editor: Theo Sommer
Editors: Peter H. Koepf, Kevin Lynch, Lutz Lichtenberger

Senior Art Director: Paul M. Kern
Layout: Manuel Schwartz, Mike Zastrow

Times Media GmbH
Tempelhofer Ufer 23-24
10963 Berlin, Germany
www.times-media.de
info@times-media.de
Phone +49 30-2150-5400
Fax +49 30-2150-5447

ISSN 2191-6462

Press deadline: November 1, 2013

Yes, we can – but should we?

The blowback from NSA spying on foreign leaders could damage American security | By Michael Hayden

During the 2008 US presidential race, the Obama campaign was near legendary for its mastery of the digital world and the candidate himself was a near obsessive user of his Blackberry.

After the election, President-elect Obama expected to be able to continue to use his personal device, telling CNBC, "They're going to have to pry it out of my hands."

All that was much to the alarm of those responsible for protecting him and his communications (and presidential records).

Eventually a compromise was reached. The president kept his Blackberry, his e-mail list was confined to a small group of family and friends, and the device itself received some security enhancements.

The episode is instructive as we now read a daily dose of allegations that the National Security Agency is reading the email or tapping the cellphones of foreign leaders from Mexico to Germany.

Visualize the backdrop against which this little episode played out in early 2009. The most powerful man in the most powerful country on earth was warned that his communications were vulnerable to intercept by foreign intelligence services in his own national capital.

No attempt was made to portray this as anything other than the way things are. No moral offense, no political pressures, no public posturing. Implicit was the belief that if our president's communications were stolen, shame on us.

Equally implicit was the belief that in gathering foreign intelligence, other nations were quite active.

As was the United States. Starkly put, absent political guidance to the contrary, if you are not protected by the US Constitution and your communications contain information that would help keep America safe, information not otherwise available to the US government, the default option would be to target your communications.

Now that's an admittedly hard edged view to inject into the current discourse over alleged American spying on foreign leaders.

But that needs to be included, even as we weigh other important factors that should also be considered. Factors like good friends shouldn't put their partners in politically impossible situations.

Recent reports in the French paper *Le Monde* and the German weekly *Der Spiegel* may or may not be true (Director of National Intelligence Clapper hammered the *Le Monde* report for its inaccuracies). German, French or Mexican leaders may or may not have already suspected such activities were going on.

Little matter. The issue now is that seemingly plausible reports of American espionage against senior foreign leaders are in the public domain, and publics – to which these democratic leaders must be responsive – are angry and demanding action.

For foreign leaders there is necessarily at least a little theater involved here. Public allegations of specific espionage require "victims" to be publicly outraged.

But the ultimate cost could be far more than cosmetic. Intelligence cooperation with the United States, clearly in the interest of both the US and its foreign partners, may be curtailed. US businesses may unfairly be forced to suffer financial loss when competing for foreign contracts. Overall political relationships could suffer (witness the cancellation of a state visit by Brazilian President Rousseff).

General (ret.) Michael Hayden is a former director of the CIA and the National Security Agency. He is currently a principal at the Chertoff Group, where his area of focus includes technological intelligence and counterintelligence.
CHERTOFF GROUP

Merkel-NSA

President Obama seemed to be reflecting these dangers in a press conference in Sweden in June when he emphasized that "...what I've said domestically and what I say to international audiences is... just because we can do something doesn't mean we should do it."

Promising to address these issues, he added that there were "questions in terms of whether we're tipping over into being too intrusive with respect to the – you know, the interactions of other governments."

That doesn't necessarily mean dramatic changes in all American intelligence collection, but that "political guidance" factor referenced above is likely to get a lot more robust and more limiting on collection activities.

Some of that may be out of a sense of embarrassment and a concern over legacy. But it's hard to deny that continued blowback from stories like these recent ones could well damage US security in terms of foreign cooperation politically impossible to deliver.

So the President will have to do some rebalancing, in the interest of politics, policy and defense.

But he will also need to be careful.

American intelligence officials will remind him that US intelligence suffered in the 1990s when Human Intelligence collectors were told to stand down and not talk to "bad" people. It's possible to create the same effect again if we now tell Signals Intelligence collectors they cannot listen to any "good" people.

That will not satisfy some critics, in the United States or abroad, but in a world of sovereign states and enduring dangers, that is the way things are. ■

PICTURE ALLIANCE/ROPI/JOSE GIRIBAS

Op-ed Germany

Former German Chancellor Helmut Schmidt (SPD) assumes that he was snooped on during his tenure in office. Writing in the weekly Die Zeit, he said he had always had a low opinion of the intelligence services:

Everyone knows that foreign intelligence services throughout the world do things that are illegal under local law. Or, they do what the law requires but also what it does not require. That is why committees were established with the task of monitoring the activities of intelligence services. They are staffed by people who feel important but do little. I always preferred to talk directly with Nixon, Kissinger, Ford and Reagan – and with Brezhnev and Honecker as well.

I feel the current furor is artificial. Merkel was bugged. Feelings of indignation are plausible but we do not know whether any secrets were overheard and if so what they are. As a head of government she must assume that any intelligence service that has the technology is listening in on her. I would advise the Chancellor to maintain her composure.

Outrage in Germany over NSA surveillance of Angela Merkel's cell phone was matched in other countries such as Brazil, Mexico and France that were also targets of US spying.

Süddeutsche Zeitung, Munich

Did Obama know about it? If not, why not? Is his intelligence service running amok or does the US President deliberately know nothing, so he can play the innocent if his back is against the wall? We may hazard one prediction: that the value of the information the US government gained by eavesdropping on the Chancellor pales in comparison to the political damage that public knowledge of the surveillance has caused. Germany and the US could be facing the deepest rift in their relations since the crisis preceding the Iraq War.

Die Welt, Berlin

There's something extremely hypocritical about the outrage over the NSA. Everyone knows that, in this respect, German intelligence services are not radical-democratic lambs either. They collaborated with the NSA, forwarded information to the NSA and received data from them in return. If we condemn the NSA's practices, it is because our resources are inferior.

Die Zeit, Hamburg

Can we imagine Obama's huge surveillance machine giving up? Or the British and French stopping their monitoring of Germany's digital traffic? Or even the Russians switching off the sensors in their Berlin embassy? Trust is good, but verification is better. Letting out your anger is good for the soul, but upgrading your defenses is more dependable. There are a hundred ways to stop the digital snooping. That establishes respect – the firmest foundation for any friendship.

Handelsblatt, Düsseldorf

Free markets and free exchange of ideas require trust. That trust must exist not just among business partners but among governments as well. It is now in jeopardy. Obama should have recognized this danger long ago. But perhaps that is why the NSA hydra is not backing down – because it has developed a life of its own and can no longer be easily restrained.

Should talks on the transatlantic free trade zone be suspended? SPD parliamentary leader Frank-Walter Steinmeier in the Frankfurter Allgemeine Sonntagszeitung:

The greatest damage is the loss of trust. We are negotiating with the Americans over free trade between the United States and Europe. That's a very big project. That is why these negotiations require a great amount of trust on both sides. I see major difficulties in bringing these talks to a successful conclusion if we don't finally establish clarity over US monitoring practices.

FDP leader Christian Lindner wrote in the Frankfurter Allgemeine Zeitung:

Without a transatlantic privacy agreement, transatlantic free trade talks are pointless. (...) The US has at least as strong an interest in intensifying trade relations as Europe, so issues of commerce and civil rights have to be packaged together. In technological reality, "Big Brother" and "Big Data" work hand-in-hand anyway. Europe can stand up and say: freedom comes before free trade.

Unfriendly fire in cyberspace

The effrontery of NSA surveillance of US allies is as staggering as its scale | By Theo Sommer

For more than sixty years, mutual trust was the cement that held the Western alliance together. The revelations by Edward Snowden of America's maniacal eavesdropping not only on its potential adversaries and rivals but also on its closest friends in Europe have caused a dramatic crisis of confidence. Wiretapping Angela Merkel's cellphone turned out to be the last straw.

An outraged German chancellor called the US president to express her displeasure, while her spokesmen complained publicly about a "serious breach of trust" and "totally unacceptable practices." Between close partners, their message ran, surveillance of a government chief's communication should be taboo.

Two years ago, when Obama conferred the US Medal of Freedom on Merkel, he extolled her "eloquent voice for human rights and dignity around the world." He praised her commitment to freedom, which "must be struggled for, and then defended anew, every day of our lives." And he praised her especially for having refused to spy for East Germany's secret police, the Stasi.

The question now is: Was the NSA listening in when she rang Berlin after that solemn award ceremony? Washington's ambiguous assurance when news of the scandal broke, that she "is not" and "will not" be monitored allows the conclusion that at the time she clearly was – apparently she had been spied on since 2002.

Theo Sommer is the executive editor of The Security Times and The Atlantic Times and Editor-at-Large of the German weekly Die Zeit.
ARCHIVE

Merkel-NSA

Merkel's indignation is all the more understandable given her reaction in June, when Snowden's leaks were first published: She said she had no reason to believe that she was being monitored. Asked in her office by journalists from the German weekly Die Zeit whether she was sure, the chancellor replied: "I am confident that our experts are able to guarantee the security of these rooms."

Obviously, it never crossed her mind that her mobile phone, her preferred instrument of communication, was not secure. At the time, she asked Washington for explanations, but not too insistently. Quite naively, she believed the assurances of a US agency whose director, James Clapper, as was already known at the time, had brazenly lied to a Senate committee. Her interior minister denounced criticism of American data mining as a mix of anti-Americanism and naiveté, and her chief of staff declared: "The allegations are off the table; this issue is over." Famous last words.

In the meantime, it has become obvious that the German government was lied to for months – a circumstance that it meekly tolerated. In retrospect, the accusation by Peer Steinbrück, then the Social Democratic candidate for chancellor, that Merkel had violated her oath of office by not energetically enough averting damage to the German people, sounds painfully plausible. She did not react when millions of Germans were affected – but she flew off the handle when her own cellphone was tapped.

SPD Chairman Sigmar Gabriel put it this way: "She defends the interests of the US secret services rather than the interests of German citizens." Aware of the harsh strictures directed at her on this account, Merkel changed tack.

"Spying on friends, that won't do at all," she declared and "this is not merely about me but about each and every citizen. It's about trust and confidence amongst allies and partners, which must now be restored again." Volker Kauder, the majority leader of her party in the Bundestag, put it more bluntly: "Obama can't go on like this."

Restoring trust and confidence won't be easy. Not because the Germans are overly sensitive about their past – the Nazi Gestapo and the Communist Stasi – but because they are worried, as are more and more Americans, about the encroachments of the 16 US secret services on the hallowed civil rights anchored in the Fourth Amendment to the US Constitution. For Germans, the constitution of America's Founding Fathers has been an inspiration and a model that they have been emulating since 1945. They are concerned that it is now being hollowed out by intelligence agencies running amok.

It is one thing to track the communications of people suspected of links to international terrorism – incontestably a cautionary necessity; or to spy on adversaries or geopolitical rivals – they all do that, first and foremost China and Russia, and counter-espionage is not only natural but permissible. But the NSA's vacuum-cleaner approach is something entirely different. Targeting friends and allies is disrespectful, indefensible – obnoxious.

The effrontery of the NSA's electronic spying is as staggering as its dimensions: The agency bugged the EU embassy in Washington; it tapped the offices of the UN Secretary General; from its premises in NATO's nearby headquarters it spied on the EU Commission; it collected, stored and analyzed huge amounts of data in France, Spain, Italy and elsewhere, 500 million data sets in Germany alone. The heads of state or government in 35 countries were on its target list, amongst them Brazil's President Dilma Rouseff and Mexico's President Enrique Pena Nieto. According to the most recent revelations, the NSA has been amassing and sifting seven million French data sets every day – phone calls, e-mails and text messages, including the communications of the Quai d'Orsay, of prominent businessmen, politicians and public servants. In 80 places around the world – including Berlin – US embassies have been abused as digital spy centers.

Something has gone terribly wrong here. Prism and other data mining operations have become

> The digital overlordship of the NSA has caused a grave crisis in the Atlantic Alliance.

a perversion of anti-terrorism. Only paranoid minds can hatch the idea that seizing close to 100 billion communications every month makes the US safer, more popular and more respected in the world. The risk–benefit analysis just doesn't make sense. The NSA's avowed goal of "total information awareness" divorces dominion over information technology from accountability for its use. It demoralizes the democratic political process.

President Obama is said to have told Chancellor Merkel that he did not have the slightest idea she had become the victim of his Special Collection Service. It had apparently been tapping her cellphone since 2002 – and in all likelihood the phones of her more important ministers as well. A plausible denial? Even before then, many European observers had reached the conclusion that Obama was either a liar and a hypocrite or that he had lost control of his bloated intelligence apparatus. It's hard to say which would be worse.

"In the war against transnational terrorism, the Obama administration has lost all sense of proportion," wrote the conservative *Frankfurter Allgemeine Zeitung*. "It is obviously no longer able to distinguish friend from foe." Writing in the French daily *Le Monde*, French lawmaker and intelligence expert Jean-Jaques Urvoas complained: "The US has no allies, only targets or vassals." In Britain, *Guardian* columnist Timothy Garton Ash quipped: "The quantity and intimacy of what the spooks and companies know about you and me outstrip a Stasi general's wettest dream..."

The point here is not that Obama's credibility has reached its nadir in Europe. Once idolized in Germany, he is now seen as a weak performer. Angela Merkel thinks he is an overrated politician, according to *Der Spiegel* magazine, long on speechifying yet short on delivery, unreliable and lacking any feeling for his allies' sensitivities.

In the eyes of many Europeans the gigantic scale of America's clandestine operations undermines America's soft power. Abu Ghraib, Guantanamo, waterboarding and extraordinary rendition had already cast dark clouds over the City on the Hill. The two wars in Iraq and Afghanistan, won militarily but lost politically, and the intervention in Libya, where Washington led from behind into foreseeable chaos, have damaged US strategic credibility.

At the same time, the American brand of capitalism has twice within a single decade precipitated the world into a grave economic crisis. And with gridlock now the hallmark of the US political system, many feel Washington has forfeited the right to tell others what to do and how to do it.

The Nobel Peace Laureate president's drone warfare is earning much criticism. Now, the James Bond excesses of Obama's espionage establishment belie his campaign promise to "lead the world by deed and by example."

There is no denying the fact that the digital overlordship of the NSA has caused a grave crisis in the Atlantic Alliance. No one should be surprised that Europe will take measures to forestall similar encroachments on its sovereignty in the furture. The European Parliament has already voted to suspend the Swift Agreement which allows the sharing of banking data with the US. Its president, Martin Schulz, went even further, calling for the suspension of the EU-US negotiations about a transatlantic treaty on free trade and investment.

His call is unlikely to be heard, but the Europeans will surely refuse to sign any treaty that does not explicitly protect the privacy and the "informational self-determination," as the German constitution puts it, of their citizens. And they will not only make US digital giants like Google, Facebook or Microsoft pay taxes in the EU, but also require them to get approval from European regulators before releasing any data on EU citizens to American intelligence agencies.

Ensuring transparency is now the order of the day. One immediate objective is a no-spy agreement with Washington, which the French and the Germans are to negotiate on behalf of the 28 EU member states, hopefully finishing before Christmas. But beyond such an agreement – which, who knows, might be honored more in the breach than in the compliance – other ideas are abroad to protect the privacy of European citizens and safeguard the business interests of European companies.

Measures under discussion include: speeding up the conclusion of an EU data protection agreement; "national routing" so mails can bypass the US and the UK; a separate "Web 3.0" that would grant Europeans freedom from unwarranted US surveillance; acceleration of the Galileo project to gain independence from the Pentagon-dominated GPS system: even closing down NSA or CIA installations in continental western Europe; and, last but not least, strengthening Europe's defense, deterrence and offense capacities in cyberspace. Technical sovereignty is the new watchword.

The short-term damage of the "handygate" spying scandal is enormous. (The German word for cellphone is "handy.") Yet the United States and Europe still need each other. They would be foolhardy if they allowed the ongoing continental drift to separate them even further. A US apology, sacking some NSA culprits and the candid presentation of the facts could help a great deal to calm the waters. For the rest, all Western leaders should take the wise counsel to heart which Lawrence Fink, CEO of BlackRock, offered America's politicians to mend their dysfunctional political system: a return to good faith, civil deliberation and mutual respect. ■

PICTURE ALLIANCE/AP PHOTO/MICHAEL SOHN

The spying continues

The German government must act to shield its citizens' data from foreign surveillance – A view from the opposition benches | By Hans-Christian Ströbele

PICTURE ALLIANCE/DPA/BORD HANS-CHRISTIAN STRÖBELE

German opposition lawmaker Christian Ströbele (Greens) with NSA whistleblower Edward Snowden in Russia on Oct. 31.

People, companies and authorities in Germany are worried. Reports and files supplied by whistleblower Edward Snowden show that foreign intelligence services, above all the National Security Agency (NSA), have tapped into millions of calls and electronic conversations within Germany and continue to suck up, store and scrutinize many more.

Since June, new details have been coming to light on an almost weekly basis. Many have yet to be acknowledged and properly investigated. The German government has disputed mass surveillance of data flows within Germany. It is undisputed that German data traffic routed through servers and the big Internet providers in the US as well as via fiber-optic hubs in the UK is being monitored and stored – maybe even in the US embassy in Berlin?

The German government and Chancellor Angela Merkel herself promised a quick and thorough investigation. They sent written inquiries to the US and Britain. We do not yet know how or whether these were answered. They held talks and sent delegations, yet the chancellor and her ministers have shied away from asking for specifics and demanding replies.

Instead, they announced negotiations on a "no-spy" agreement. But in the meantime the spying continues. Merkel's government has yet to act to put a stop to it.

The German government's foremost duty is to protect the country's people, businesses and authorities from harm, including shielding their data from foreign snooping. The government must insist vigorously that the US fully account for its actions. It must demand answers on whether the NSA, using its Prism and XKeyScore software, has sifted through hundreds of millions of electronic transmissions by Germans that it received from companies like Google, Facebook, Skype, Yahoo and AOL.

From its EU partner Britain, Germany must insist on answers to whether, together with the NSA, the Government Communications Headquarters (GCHQ) intelligence service really is using its Tempora software to tap transcontinental undersea cables that carry much of the world's data traffic. It must leverage EU institutions to stop these adversarial, even hostile practices that contradict the letter and the spirit of the EU treaties.

Hans-Christian Ströbele is a Member of the Bundestag for the opposition Greens. He sits on the Parliamentary Oversight Committee, which monitors the activities of Germany's intelligence services.

ANDREAS WEEGER

Merkel-NSA

The government must clarify whether and to what extent Prism and Tempora are being used for purposes of corporate espionage. Monitoring of EU offices, German ministries, embassies, authorities and companies violates data protection and criminal laws.

German prosecutors must probe these allegations, using Snowden's files as their foundation. They must – using current law enforcement treaties – demand information from the US and Britain and interview Snowden as a witness.

This could be done in Moscow. It would be preferable, however, if Snowden and his documents were available to German law enforcement. To make that possible he should be granted free passage, a German visa and witness protection. Doing so would also be appropriate on humanitarian grounds, because Snowden's revelations have done a great service to human and civil rights worldwide and in Germany.

He has said repeatedly that he would be available as a witness to further investigations. So far no court proceedings have been opened. The German government should champion this cause.

The government must also ensure, through guidance and prohibitions, that German authorities do not use data about the German people collected through illegal surveillance. Communications data that has been covertly collected, stored and analyzed without a court order or parliamentary control is tainted. Its use is forbidden in Germany, as is all other information that has been gathered illegally or by criminal means.

German intelligence services are not permitted to circumvent German law by gathering and using information on Germans obtained from US or British intelligence. Other German authorities may not analyze such data if it is offered to them by the US or the UK.

The same applies to citizens of other states if, according to their laws, data was collected illegally – for instance by the NSA sifting through the contact lists of hundreds of millions of e-mail and messaging customers illegally and without the authorization of the secret US Foreign Intelligence Surveillance Court (FISA).

The German government must re-negotiate agreements on the presence and stationing of foreign armed forces in Germany, especially the NATO Status of Forces Agreement and its supplementary pacts. The goal must be to ensure that foreign troops in Germany must verifiably and without exception observe German law.

In particular, agreements must be negotiated with the US and Britain that communications data on German citizens may only be collected, stored and analyzed in accordance with all formal and practical restrictions in Germany, which also apply to Germans abroad. Judicial and parliamentary oversight must also be applicable.

Internationally the German government should insist on binding and tough privacy protection standards in global data traffic. Article 17 of the International Covenant on Civil and Political Rights, which, like Article 8 of the European Convention on Human Rights, protects privacy and personal information, could be structured accordingly; safeguards should be agreed between the EU and USA as part of the future Transatlantic Trade and Investment Partnership (TTIP) agreement and its conclusion made provisional to a binding "no spy" agreement. Current EU data protection legislation should be revised to include a provision that data transfers to the US and non-EU states with low data protection standards through companies such as Facebook and Google must be licensed by European supervisory authorities.

The German government should act to suspend and re-negotiate the Safe Harbor agreement with the US, because in the United States there is no comparable data protection guarantee for Europeans. Berlin should also move forward with a breach of contract complaint against Britain because of its Government Communications Headquarters, if the EU Commission does not.

The German government should broadly support the continued development of easily accessible technological protection standards against data leakage. Those who encrypt their correspondence should not be placed under suspicion or surveillance as a result. US companies including CryptoSeal and Lavabit, which offer secure e-mail correspondence and have run into trouble in the US, should be offered help to relocate to Germany. ■

When in doubt, choose freedom

Cybersecurity can only be effective if it is based on fundamental rights | By Alexander Graf Lambsdorff

The NSA headquarters in Fort Meade, Maryland, has 17,000 parking spaces.

AFP/GETTY IMAGES

In history books, June 6th, 1944 has been marked as "D-Day" – the launch of the decisive military operation by the Western Allies that liberated Europe. It is quite possible that Edward Snowden didn't have this historical date in mind when he initiated his own operation exactly 69 years later. On June 6, 2013, however, he revealed an unprecedented mass surveillance that is the biggest intelligence scandal of our times. The liberators of the past, the United States and the United Kingdom, are the alleged villains of the present.

Since then, there has been a steady drip of troubling and embarrassing disclosures. The data mining by the "Five Eyes" strategic alliance of Australia, Canada, New Zealand, the UK and the USA has clearly gone overboard. The National Security Agency (NSA) and Britain's Government Communications Headquarters (GCHQ), in particular, are said to have spied on millions of EU citizens, mainly German and French. In the United States, the NSA collected masses of metadata in clear violation of the fourth amendment – framed explicitly to protect law-abiding US citizens from unreasonable searches by government agents.

Reconstructing transatlantic relations after George W. Bush left office was one of President Barack Obama's major foreign policy achievements. It may well go up in smoke if the US does not deal with the fallout from this scandal in an appropriate manner.

The latest disclosures added a new dimension to the situation. It wasn't just ordinary people's data being collected but also those of the German chancellor. When allied Western leaders are subjected to this kind of attack from Washington, and Washington gets caught due to its strangely ineffective protection of sensitive data (as already witnessed in the Wikileaks affair), a deep and serious breach of trust in the transatlantic friendship is no longer just a hypothetical contingency. It is too early to tell what the political consequences of these revelations will eventually look like but the risk of transatlantic estrangement looks more real than at any other time in post-war history.

So what can European countries and the European Union do to protect the privacy of their citizens and governments?

First and foremost, Europe has to agree on common standards of data protection and data security. Adopting the EU data protection directive must now be an urgent priority. The British and, astoundingly, the German government chose to delay its adoption until 2015.

On such a legal basis Europe could speak with one voice in the future when faced with scandals of this kind. It is a farce that Francois Hollande did not call President Obama until French citizens were affected by NSA surveillance; Angela Merkel only called Obama when she found out that her own mobile phone was a target; and David Cameron probably didn't call at all because British intelligence carried out its own operations against fellow EU member states, a clear breach of the EU treaty.

Alexander Graf Lambsdorff (FDP) is a member of the Foreign Affairs Committee of the European Union Parliament.

SABINE SCHRÜNDER

Merkel-NSA

From a civil rights perspective, an important first step was made when the European Parliament recently called for temporary suspension of the Terrorist Finance Tracking Program (TFTP) agreement, which grants US authorities access to the bank data of European citizens for terror-related investigations. This resolution was inevitable since there were clear indications that TFTP, also known as the Swift Agreement, has been abused by the NSA.

James Clapper, Director of National Intelligence, admitted that information was collected to evaluate other countries' economic policy and to be able to foresee international financial crises. But this was never the aim of the TFTP when the European Parliament gave its assent in 2010. So it is right to examine these allegations in the course of a full technical onsite investigation and to consider renegotiation where appropriate, in particular over the Safe Harbor agreement for EU data on US soil that the US signed and apparently violated.

Alongside political and diplomatic efforts, technical measures are imperative, especially since it transpired that the diplomatic missions of the EU in the US were bugged. The EU's first Cyber Security Strategy, which was launched earlier this year, comprises technical and legal proposals regarding the internal market, justice and home affairs and also foreign policy aspects of cyberspace issues. The increase in online economic espionage and its threats to EU governments and companies are explicitly dealt with.

To ensure a high common level of cybersecurity, a number of Computer Emergency Response Teams (CERTs) operate in each EU member state under the framework of the European Union Agency for Network and Information Security (ENISA). And with the launch of the European Cybercrime Centre (EC3) at Europol, a European focal point in the fight against cybercrime was established.

Cyber security can only be effective, however, if it is based on freedoms and fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union. Reciprocally, individuals' rights and freedoms can only be secured with efficient law enforcement, safe networks and systems – and authorities able to strike a balance between these fundamental rights and interests.

Werner Maihofer, a German liberal politician and legal philosopher, once said: "Total security means total restriction. Total freedom means total insecurity. The liberal position is to find the right balance. And if security and freedom are clashing: in dubio pro libertate. When in doubt, choose freedom." ■

A really Eurasian union

Russia's efforts to establish a regional power bloc are faltering | By Fyodor Lukyanov

Russia's ambivalent position between East and West, Asia and Europe is part of its national culture and an endless source of intellectual debate through the centuries. From time to time, this cultural dualism turns into a geopolitical debate about competition with other powers. Now we face another round.

This time the focus is on Kiev, prompted by the expected signing of the Ukrainian Association Agreement and the Deep and Comprehensive Free Trade Agreement (DCFTA) with the European Union. The atmosphere surrounding this event, due to take place in Vilnius in late November, has been quite overheated as both Russia and the EU have blown up a routine bureaucratic procedure into a geopolitical Rubicon. However, everyone agrees that the Vilnius meeting will mark a new stage in the development of what is habitually called the post-Soviet space.

In Russia we used to think that our neighbors were torn between the choice of Russia and someone else – Europe, China, America. But now Russia itself faces a serious choice: Moscow has to decide how far it is ready to go in the name of President Putin's integration project, the existing Customs Union (Russia, Belarus, Kazakhstan) which he wants to transform into a Eurasian Economic Union by January 2015. To what extent is Russia ready to make concessions today for the sake of building an association that may yield dividends in the future?

There is one more important point. If Ukraine really enters on an EU path that will rule out its institutional rapprochement with Russia (which everyone is now talking about), the union Moscow is lobbying so hard for may never turn out the way it was planned.

It is no secret that the most serious integration projects of Russia – the Common Economic Space and the Customs Union – were launched largely with an eye to Ukraine; for economic and, especially, geopolitical reasons. While Kiev's membership was not ruled out, the project's name – "Eurasian Integration" – was rather far-fetched. Of the four core members of the planned association, only Kazakhstan is really part of Eurasia, while the other three are oriented towards Europe – not the EU but Europe's cultural, historical and geographical area.

If Ukraine is ruled out, the "Eurasian" nature of the project becomes more real. Its main vector would be toward the east and southeast. The question is, of course, how much this orientation would find acceptance in Russian society, which has been swept by anti-immigrant attitudes and is prone to cold-shouldering Asia.

But Ukraine's absence would have one more consequence. Any association that provides for joint decision-making and the partial secession of sovereignty needs to establish an internal balance. All members must be confident that by delegating their rights they will not become targets of discrimination. Such guarantees must be bolstered, above all, by the association's institutions and a system of checks and balances that ensures equal opportunities for all.

When European integration began in the 1950s, its founders – France, Germany, Italy and the Benelux countries – were roughly of equal size. Post-Soviet integration involving Russia dooms the project to an inherent imbalance – all its possible partners are significantly inferior to it in the economic, political and demographic scope.

Of course, Ukraine would not be an equal counterweight to Russia, yet the overall balance would be different if it joined. After all, Ukraine is a country with a population of more than 40 million, with a potentially strong economy and a very unyielding political mentality. Strangely enough, the absence of such a state in the association will be a problem for the strongest member as it would be feared by all the others on account of its sheer weight.

Grigory Marchenko, one of the most respected economists in the former Soviet Union who has just resigned as president of the National Bank of Kazakhstan, recently discussed this issue in a televised interview. Speaking to Russia 24 TV channel, he said that "neither Ukraine nor Turkey will be able to fully integrate into the European Union. Therefore they both should be invited to the Customs Union, where the decision-making process should be built in such a way that they would not be afraid that Russia would dominate and that their interests would not be taken into due account."

Kazakhstan and Belarus are also concerned about the equality problem. In this context, Marchenko came up with an even bigger idea. He said the Customs Union should be extended by association agreements with China and Mongolia. "Then there will be a basically different critical mass and basically different relations both within the Customs Union and with European neighbors."

It requires a bold flight of fancy to imagine a Customs Union uniting post-Soviet countries as well as Turkey and China. But it is easy to imagine whose goods would dominate in that common market. Yet Marchenko's train of thought is understandable – as things stand now, a transition to a qualitatively deeper integration is unlikely. But if real heavyweights are added to the Union, the smaller countries will have more room to maneuver.

Ukrainian President Alexander Lukashenko expressed the opposite view. He is against the Union's enlargement in principle (Armenia and Kyrgyzstan are the most likely candidates) unless the three founding members build an efficient mechanism to ensure equality for all. But if genuine equality is not achieved, the value of integration will be low.

Russia faces a difficult dilemma: It is too large and has too obvious an expansionist history to implement a regional integration project without causing fear among its neighbors. At the same time, it is not large enough (economically and in terms of influence) to overcome the resistance of other centers of power and to delineate its own stable orbit. This is still possible in the security sphere – the Georgian War has stopped NATO's enlargement – but it is not likely when it comes to the creation of a space of norms and rules that would attract others.

Moscow's ability to counterbalance rival centers, be it the EU or China, is limited. Its efforts to prevent the withdrawal of potential ex-Soviet partners may fail, as seems to be happening with Ukraine. The alternative is the construction of a joint space with some of the other centers. But then Russia would have to defend its own right to equality.

"Co-creation" with the West is hardly possible, as the EU offers integration only on its own terms, that is, if others adopt ready-made European norms and rules. In the East, there is more room for flexibility – norms and rules there will be created anew. At the same time, it will be difficult to defend one's vision there if Russia assumes in earnest that major states such as China or Turkey will participate in the project.

There is also an idea to form a bridge between the two large areas of integration, laid down in policy in several documents, including Putin's article two years ago, in which he launched his Eurasian integration project. But there is no formula for its practical implementation. It is too abstract.

Fyodor Lukyanov is editor-in-chief of the journal Russia in Global Affairs.

PRIVATE

Russia

When the Eurasian project first emerged, things seemed much easier. Russia, which had just recovered from a geopolitical shock, wanted to restore what it could of its former glory in the old Soviet territory. But precisely this has turned out not to be possible. On the other hand, Russia's self-identification depends on this project's future.

It might come to pass that, as a result of the successful implementation of the Eurasian integration idea, Moscow will not be the main capital of Eurasia but will have to yield first place to Beijing or Ankara. Then Moscow might turn back to Europe for a counterweight to the emerging Eurasian giants. ■

Strategic considerations: Russian President Vladimir Putin playing billiards.

PICTURE ALLIANCE/DPA

continued from page 1

Call of duty

Finally, from the point of view of many younger officers in particular, this fragmentation is also far removed from the operational needs they have experienced in Afghanistan and other missions over the past ten to fifteen years. For them, having served together with many NATO partners, interoperability on the ground is absolutely essential. Effectively, we are failing our soldiers so far in this regard.

The European governments are aware of the ineffective and inefficient use of defense expenditure. They are just as aware of the conclusion that significantly greater cooperation on defense is the only way of addressing this problem. This realization is reflected in the initiatives of Pooling and Sharing in the European framework, and Smart Defense in the NATO framework. Hardly a talk is given or a declaration signed where the importance of more cooperation is not stressed.

For example: The Franco-German declaration of Feb. 6, 2012 states that "In times of strategic uncertainty and limited resources, strengthened defense requires common procurement. As a consequence, we must be ready to take the necessary decisions."

But what are the necessary decisions? Where are the ideas? Who is moving ahead? Up to now only one thing is clear: that not nearly enough has happened.

In certain areas – the European Air Transport Command (EATC) is a good example – progress has certainly been made. But why not think bigger? Why not, for instance, have a European fleet in the Baltic?

Of course, we are still a long way from far-reaching decisions regarding specialization or full integration. Ultimately, this affects an area that has, for centuries, been at the heart of national sovereignty – and one that brings with it many difficult and uncomfortable questions.

And yet to conclude that we should forgo all ambition, strikes me as too short-sighted. The Dutch Defense Minister, Jeanine Hennis-Plasschaert, a significant voice in the European debate, posed the question correctly at the 2013 Munich Security Conference: "Should we really fear the loss of sovereignty? Or should we rather define the concept of sovereignty in a less traditional way?"

In other words: What is the worth of sovereignty, traditionally understood, if an individual European state is no longer in any way capable of action on its own? Would not such sovereignty be meaningless?

If just a tiny step forward is made at the European Council meeting in December, this will be too little as far as European defense integration is concerned. We need ambitious goals. The European Council should also commission, in particular, an EU White Paper on Security and Defense Policy. The world – and we Europeans – want clarity about the goals, instruments, and methods of European security policy. Moreover, the German government could and should push ahead courageously in questions of majority decisions concerning foreign policy. After all, we have absolutely nothing to fear from the majority of the small EU member states – quite the opposite.

Finally, none of this means that our alliance with the US will be any less meaningful in the future. The US is making it clear how important a functional and united Europe is for them, too. To quote Vice President Joe Biden, from his speech at the Munich conference earlier this year: "A strong and capable Europe is profoundly in America's interest, and I might add, presumptuously, the world's interest."

Making Europe stronger and more capable – that would truly be a worthwhile slogan for the new German government. Incidentally, the preamble of the German Basic Law still provides the best basis for German foreign and security policy today: "to promote world peace in a united Europe."

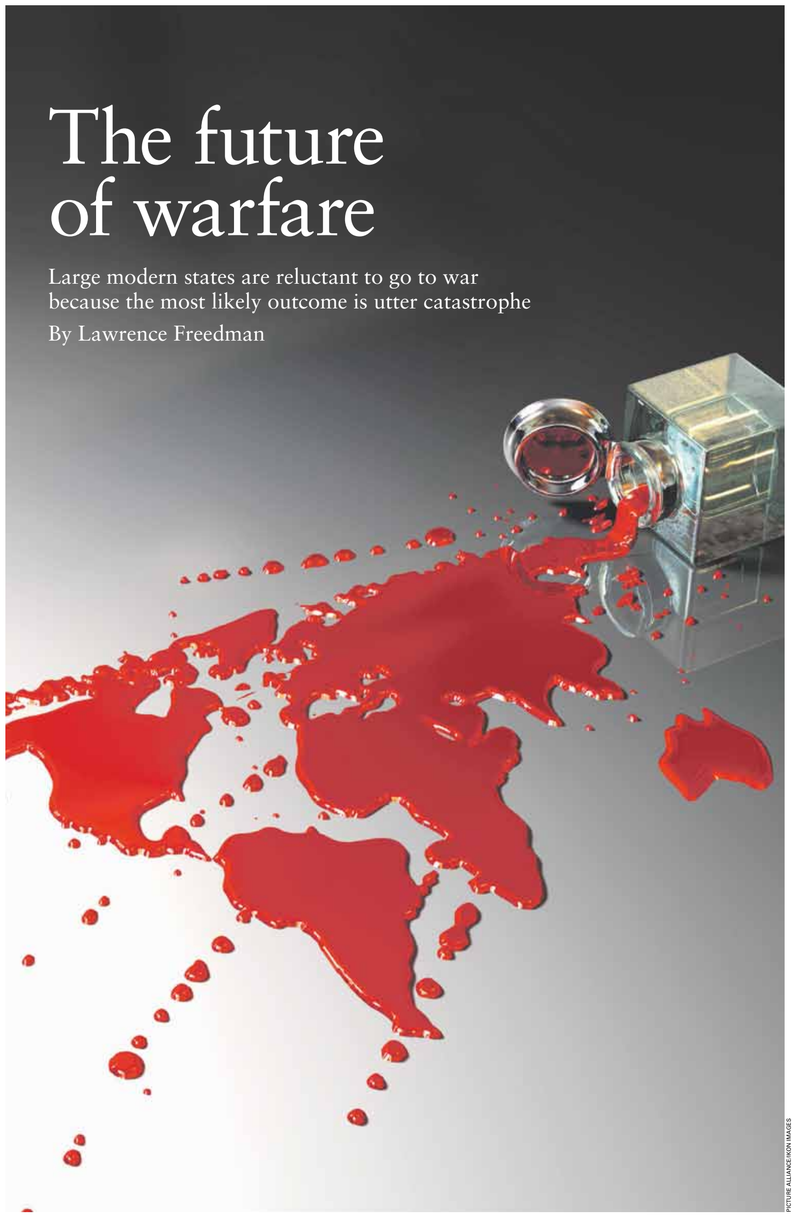
The center-right Christian Democrats electoral program from 2013 states: "In the long run, we strive for the establishment of a European army." The Social Democrats take a similar view, as indicated, for instance, by Sigmar Gabriel's speech to the German Armed Forces Staff College in Hamburg in July 2011, when he said: "We should push forward a concrete project […]: a joint European army." Just because a goal is "long-term" does not mean it can be put on the back burner.

The new German government now has an excellent opportunity to emphasize and push this very issue, beginning at the European Council in December, and to keep it high on the agenda. That would not only be beneficial for Europe. It would also be a clear and very welcome sign that Berlin is ready to further accept its central responsibility for peace in and around Europe. ■

The future of warfare

Large modern states are reluctant to go to war because the most likely outcome is utter catastrophe

By Lawrence Freedman



PICTURE ALLIANCE/IKON IMAGES

Big wars, fought between the world's greatest powers from the rise of Napoleon to the collapse of communism, are now fortunately a thing of the past. They are now spoke of as "old" wars and there are good reasons to suppose their obsolescence. There is now little sufficiently existential to be worth fighting about. Well-developed forms of dispute resolution exist. And, most important, it is well understood that should fighting begin the most likely outcome will be utter catastrophe.

Optimists note that the various reasons why nations once went to war , from imperial rivalry to ideological competition, have played themselves out while the growth of international trade and finance has created new forms of inter-dependence that encourage cooperation.

The great powers became involved in a number of wars after1945, and were at times close to combat with each other, if only through proxies. But the cold war never turned hot in part because of the prospect of "mutual assured destruction."

It has been argued that instead of the "old", great-power, industrial-scale wars we now face "new" wars, eruptions within fragile states fought between antagonistic communities or in rebellion against corrupt regimes. They tend to involve irregular forces, fighting with each other or against the regular forces of the state.

There is nothing really "new" about such wars. Throughout history societies have torn themselves apart with considerable violence, as local disputes and rivalries have become unmanageable. Such violence often peters out through exhaustion. On occasion one side prevails, with perhaps a regime overthrown and replaced. Sometimes these conflicts never quite end and societies suffer recurring disorder. Such wars therefore represent continuity rather than novelty in human affairs.

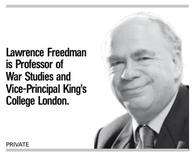
What has changed is how they have caught the attention of major powers. Once the colonial powers understood the difficulties of holding onto territory in the face of a hostile local population, interventions tended to reflect the strategic imperatives of the Cold War. Then the American experience in Vietnam during the 1960s and the Soviet Union's during the 1980s in Afghanistan warned that substantial interventions were unwise in support of regimes with limited popular support in countries imperfectly understood and against patient and resolute enemies.

After the end of the Cold War, the break-up of the former Soviet Union and Yugoslavia added to the many new states that were once part of the former European empires. Many were deeply divided and became the settings for brutality and cruelty, potentially affecting their wider neighborhoods.

No longer preparing for "old" wars, the established powers had more capacity to engage with these conflicts. For a while they did so because of genuine humanitarian concerns, aspirations to strengthen the institutions and economies of the weak states, or concern that they might turn into sanctuaries for extreme and in some cases fanatical political movements. The "new wars" literature was prompted by the period of regular intervention that began with the Gulf War in 1991, and peaked during the 2000s with the campaigns in Iraq and Afghanistan.

The novelty, therefore, lay in the number of states susceptible to internal conflict and the unprecedented degree of external meddling. Western armed forces became very busy with these interventions and had to learn, or re-learn, forms of warfare quite different to those geared to states with military establishments similar to their own.

The results were mixed. There were successes where vulnerable populations were protected after suffering extreme violence. But when external forces faced armed resistance with a degree of popular support, their role became increasingly circumscribed and contentious. Opponents who could lose themselves amongst the people had to be dealt with using levels of discrimination that would be irrelevant in battles between regular forces.



PRIVATE

Lawrence Freedman is Professor of War Studies and Vice-Principal King's College London.

Conflict resolution

For the moment intervention is in decline because of the frustrating and painful experience of the past decade and evident fatigue amongst the populations of the serial interveners, notably the United States and Britain. These interventions were always discretionary and required governments to make a compelling case to sustain political consent at home. This became harder in the face of casualties and without obvious political progress.

Should it be deemed necessary to take punitive action against a cruel regime or terrorists using chaotic societies as bases from which to mount attacks across borders, then the current preference, drawing on the development of classes of weapons that offer high accuracy over long distances, is to engage in either symbolic strikes or even targeted assassinations. The problem with such methods is that whatever their short-term effects, they provide no basis for the imposition of a political settlement. Thisre-quires land forces. The experience with Syria shows how in addition Russia and China remain reluctant to allow any UN authority to interference in the internal affairs of even the most brutal states.

If engagement with "new" wars is in decline might there be a revival of "old" wars? It is not hard to list the reasons why such wars would be foolish and counter-productive, especially if the belligerents were both nuclear powers, setting successful societies back by decades, their civil and economic achievements in rubble and their populations depleted and traumatized.

Were fighting to begin for whatever reason between such states they would have an interest in avoiding escalation and keeping a war limited. However, such restraint has not been tested. Perhaps conflict between states with smaller nuclear arsenals, and less-developed crisis management might lead to more risk-taking. Even after they both tested nuclear weapons in the late 1990s, Pakistan and India have been close to war a couple of times.

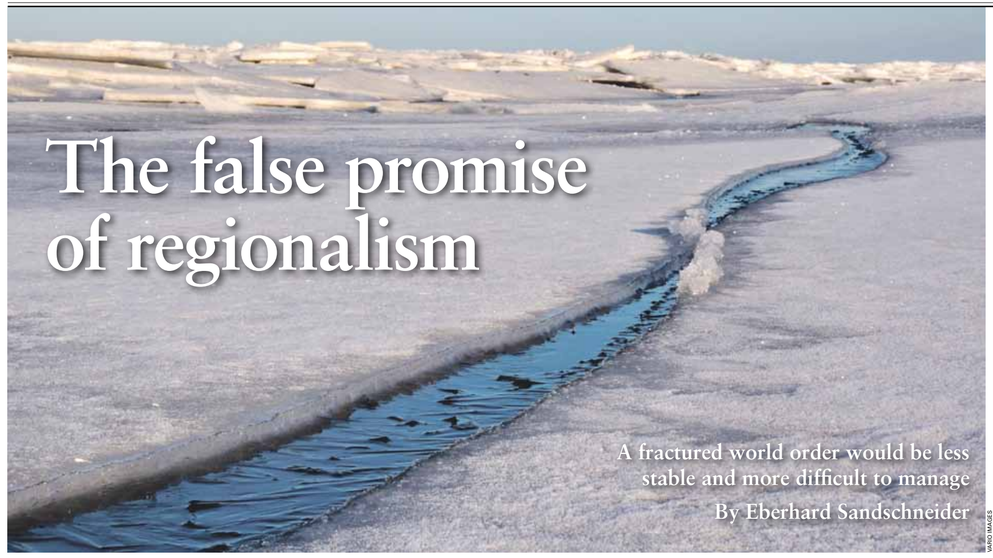
Most commentators would suggest that the most probable (which is not to say likely) setting for wars between major powers would be the Asia-Pacific region. There are, for example, worrying levels of antagonism, fuelled by nationalism, between China and Japan with an ongoing dispute over the Senkaku/Diaoyu islands. If either side used armed force, then matters could soon get very dangerous. But the most important development would be if the United States weighed in on the side of its ally, Japan. This could lead to a clash between two nuclear powers on a matter one side considers to be a vital, territorial interest and which raises for the other the integrity of its alliance commitments.

The question of a future war is to a large extent one about the future of international politics. New weaponry, from nuclear bombs to "smart" drones, opens up new ways of causing death and destruction, or of applying force in some smarter, more precise manner. But the key questions still revolve around what people believe to be worth fighting about, including humanitarian outrage, threats to values as well as territories, and treaty obligations. ■

The false promise of regionalism

A fractured world order would be less stable and more difficult to manage

By Eberhard Sandschneider



VARIO IMAGES

Regionalism is not a new phenomenon in international relations. Regional cooperation and conflict have always been defining aspects of historical developments both on the national and global levels. But in recent years, the importance of new forms of regional cooperation and coordination has come to be regarded as a new defining feature of global politics. But the risk of regional organizations threatening effective forms of global governance is more than obvious.

As European nations have made the biggest progress in regional integration, most Europeans believe in the importance of integrated global governance and global institutions. Most Europeans certainly believe in the necessity to reform the United Nations in order to improve the quality of global governance.

Saudi Arabia's leadership doesn't. The Saudi government recently became the first to decline a non-permanent seat on the United Nations Security Council, criticizing UN powerlessness and its inability to act over Syria. The Saudis are not the only ones to fundamentally challenge Western hopes for the future of institutions that used to predominantly serve Western interests and follow Western rules.

Many emerging countries seem to be concentrating on alternative strategies. Instead of aiming for complicated, costly, slow and ultimately highly implausible reforms, they focus on building alternative institutional frameworks no longer based on rules dominated by western countries.

New power projections almost automatically lead to new forms of cooperation in the space between nation states and global institutions. When Goldman Sachs invented the acronym BRICS, the heads of government of Brazil, Russia, India, China and South Africa found the idea attractive enough to convene their own summits under the new moniker and discuss non-Western approaches to global politics.

ASEAN, NAFTA, ECOWAS, Mercosur, the OAU and the SCO not only add to the plethora of acronyms haunting the understanding of international relations, they also represent a trend toward new forms of regionalism. This could well become the defining development for global relations in the decades ahead.

From a historical perspective, however, times of increased regional cooperation have consistently been replaced by hegemonic or multipolar structures. The perpetual dream of liberal institutionalism that the world will one day be governed by regional or (even better) global networks of cooperation may well remain a dream.

Will these new forms of regionalism prevail? Even more importantly, will they help to produce global public goods at reasonable cost – if at all? One may have grave doubts.

First of all, regionalism per se is not a guarantee for the production of public goods. In most regions of the world, conflicts between states trump the capacities of conflict resolution and cooperation. Even economic win-win-situations are jeopardized when border conflicts, resource competition, historical legacies driven by nationalism and acts of symbolic supremacy plague intra-regional relations.

Second, regions are never clearly defined. Outside observers cannot rely on them as their membership and their concerns are subject to frequent change. In addition, they are constantly exposed and vulnerable to global influences, even to great power influence.

Technological changes (such as in trade and communications) can also have a disruptive impact. Therefore, most forms of regionalism are difficult to manage, their specific political and economic weight is hard to assess.

Third, most regions – perhaps with the exception of Europe – show a high degree of intra-regional diversity. Low levels of cohesion, competing identities, differences in geographical size, economic development and most importantly different political systems complicate progress toward substantive regional integration. East and Southeast Asia, in particular, prove the difficulty of policy integration between monarchies, autocracies, communist systems and liberal democracies.

DGAP

Eberhard Sandschneider is Director of the Research Institute of the German Council on Foreign Relations (DGAP).

Regionalism

Fourth, it is perhaps not surprising that in many regions levels of institutionalization are restricted to minimal forms of coordination and cooperation. As long as antagonistic controversies linger and interfere with attempts at conflict resolution, most regions will remain far from the substantial levels of integration found in the EU.

Finally, while some may regard nation states as obsolete, they remain the decisive and defining actors in global affairs. In theory, increasing regionalization may lead to a world order characterized by more stability and less hierarchy than one based on nation states. In reality, however, the instability within regions and the neglect of trans-regional cooperation may bring about an ever more polycentric world order – which by definition is less stable and more difficult to manage than multipolar, bipolar or even hegemonic structures.

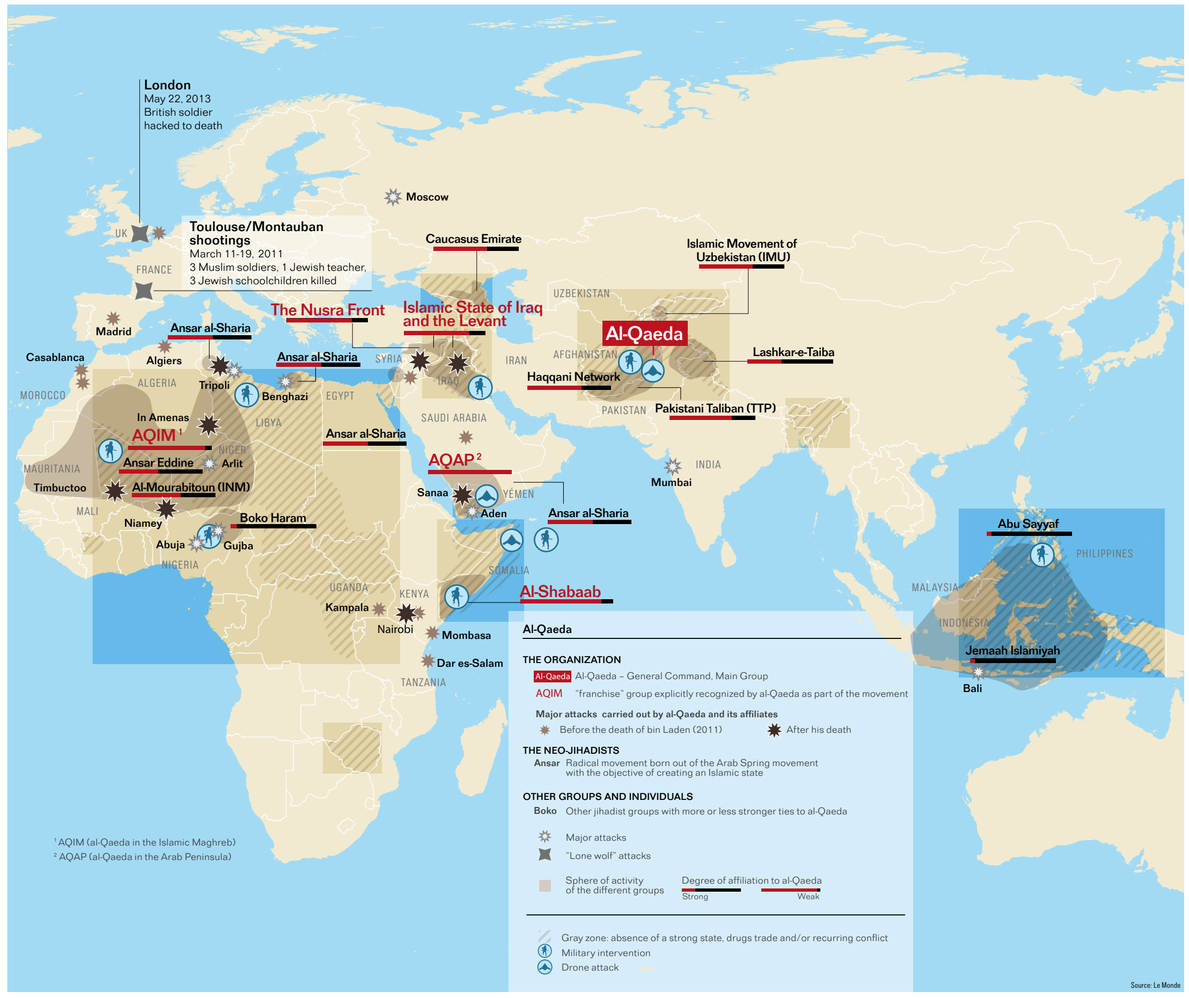
So far, several sensitive questions remain unanswered: Will the world divide up into several major trading blocs. Will weaker countries suffer from the predominance of regional powerhouses? What effects will new power currencies such as financial reserves and monetary stability have on the distribution of power within and between regions?

Global politics is far from reaching a new balance between different actors. While regional cooperation may help to reduce the levels of tension among major players, hopes for the emergence of an intermediate level of global governance are premature. Growing regionalism might well be an additional part of the problem – and only rarely part of the solution. ■

Al-Qaeda still a global threat

Exploiting instability following the Arab uprisings is currently the militant network's most important project

By Yassin Musharbash



In September 2013, al-Qaeda published a five page Arabic document called "General Clarifications for Jihadist Action." It was authored by Ayman al-Zawahiri, the Amir or leader of al-Qaeda, who had been Osama Bin Laden's deputy and became his successor after the Saudi was killed by US Navy Seals in May 2011. The document is fascinating for many reasons, but especially because it isn't addressed to a Western audience as speeches by al-Qaeda's leadership often at least partly are for propaganda purposes. Instead it is, in Zawahiri's own words, addressed to "the leaders of all entities belonging to al-Qaeda and to our helpers and those who sympathize with us" as well as to "their followers, be they leaders or individuals."

This is a large group of people. And it is noteworthy that al-Zawahiri doesn't seem to be placing a lot of emphasis on the brand name of his group. Instead everybody is invited to feel addressed. So what is al-Qaeda in 2013? An open network? Or still a hierarchical organization? Is it a network of networks? Or a system of franchise operations?

The truth is that al-Qaeda in 2013 is all of the above. Al-Qaeda can be structured as it is in Yemen. But it is also open, given that the central leadership has repeatedly asked sympathizers in the West to act in its name and on their own initiative.

Al-Qaeda's presence and influence can be obscure as is the case with the co-operation with al-Shabaab in Somalia. Or opaque, as it is in relation to various local Jihadist groups across the Arab world calling themselves Ansar al-Sharia, whose agendas overlap with al-Qaeda's. Then again, the central leadership can appear like a company's headquarters, for example when the North African branch, al-Qaeda in the Islamic Maghreb (AQIM), reprimands fighters for not filling in forms properly. Wile in other instances al-Qaeda even hides behind other names – like Jabhat al-Nusra in Syria.

At first glance this may seem erratic. But from al-Qaeda's point of view it is an asset to be able to appear in whatever form may be best at a given place or moment in time. The case of Jabhat al-Nusra, now probably the strongest faction in Syria's civil war, illustrates that: Even though the group was set up by al-Qaeda in Iraq, it didn't use that group's name so as to not alienate Syrians. Only after its support base had solidified, did the group admit to being part of the al-Qaeda nexus.

It is partly by this means that al-Qaeda over the past two years managed to establish bridgeheads in Arab countries destabilized by rebellions. In Libya and in Egypt's Sinai Peninsula for example it is quite evident that al-Qaeda plays a role – in all but name. Should al-Qaeda cadres one day feel they would benefit from the brand name, they will introduce it there.

The exploitation of the unstable situation following the Arab rebellions is currently al-Qaeda's most important project. At first the uprisings weakened al-Qaeda because the Jihadists had always claimed they would be the ones to cause the fall of the "tyrannical" Arab regimes, or "the near enemy." But this ideological defeat has since been compensated for by a huge influx of volunteers, an active role in Syria's civil war and large areas elsewhere in which the network can operate fairly freely for lack of state control.

After roughly a decade in which al-Qaeda's main interest was to plot spectacular attacks against Western targets, or "the far enemy," the pendulum is now swinging back toward the near enemy. This is not only a strategic decision by the central leadership. It is also what most new recruits are interested in.

This is not to say al-Qaeda is no longer interested in launching attacks on the West; Al-Zawahiri called for them. And al-Qaeda's branch in the Arab Peninsula (AQAP), headquartered in Yemen, is likely still devoting resources to that end. Of all groups in the nexus they have the greatest capabilities to do so. With Ibrahim al-Asiri they have a master bomb maker in their ranks who has already proven his expertise when AQAP tried to down a US jet in 2009 and two cargo planes in 2010.

Furthermore, AQAP's Amir Nasir al-Wuhayshi has recently been promoted to al-Qaeda's overall Number 2. He will want to prove his ability, and an attack outside the region is hard currency in this regard.

But the focus is now on the Arab world – and on Africa, where the expansion politics of al-Qaeda in the Islamic Maghreb, started years ago, are now paying off. In the conflict that shook Mali in 2012, AQIM's fighters played an important role, in alliance with other Jihadist networks. They have been driven out of Mali's towns since, but are still in the region.

In addition, Jihadist veteran and training networks now connect Northern Africa not only with Mali but also with Nigeria. Add to that a large number of weapons that were acquired from the Libyan army's depots, and it becomes quite clear that a string of African states in which militant Islamists are active may witness eruptions of violence instigated or supported by AQIM in the years to come.

In Somalia meanwhile al-Shabaab may be under pressure; but as the attack on the Westgate shopping mall in Nairobi, Kenya in September 2013 demonstrated, the group is capable of high profile terror attacks. They may have been helped by AQAP. But in either case there is little reason to assume that strikes like this will not happen again as long as African Union forces are fighting al-Shabaab in Somalia.

In the Middle East prospects are equally bleak. The demise of the Assad regime is clearly not the only aim that Jihadists are pursuing in Syria. They want to establish an Islamist proto-state; and they are enthusiastic about the proximity to Israel. Approximately 6,000 non-Syrian Jihadists are currently in the country, many have battlefield experience. They constitute a troubling long-term problem in any scenario. Concerns over what they may plan to do in the future are rising in Jordan, Lebanon and Turkey – even more so as al-Qaeda in Iraq is perpetrating mass casualty attacks at almost the rate seen in 2005 and 2006 while at the same time maintaining a presence in Syria.

In Egypt another pressing issue exists: Since the military unseated President Mohamed Morsi in July 2013, Islamists there feel disenfranchised. Al-Qaeda is interested in winning them over. It is partly for this reason that al-Zawahiri in his "guidelines" portrays al-Qaeda as a group that will not use excessive violence and has a clear agenda. Egpytian Muslim brotherhood supporters are not natural allies of al-Qaeda, but a more focused, more civil version of that group may be attractive to some.

A lot has been written in the past few years about the alleged end of al-Qaeda. Certainly, the US drone campaign has killed many important leaders and diminished the group's capabilities. But al-Qaeda is once more proving to be very resilient – because it is able to adapt. Just as it did, for example, at the beginning of the Afghanistan war when the group all but gave up its safe haven and ordered most cadres to go back to their home countries to continue the project from there. This is how AQAP and AQIM came about.

We are presently witnessing another transformation, as al-Qaeda not only shifts focus but also allows for more co-operation and integration with local groups at the expense of micro-management by a central leadership, which can't be maintained under these circumstances.

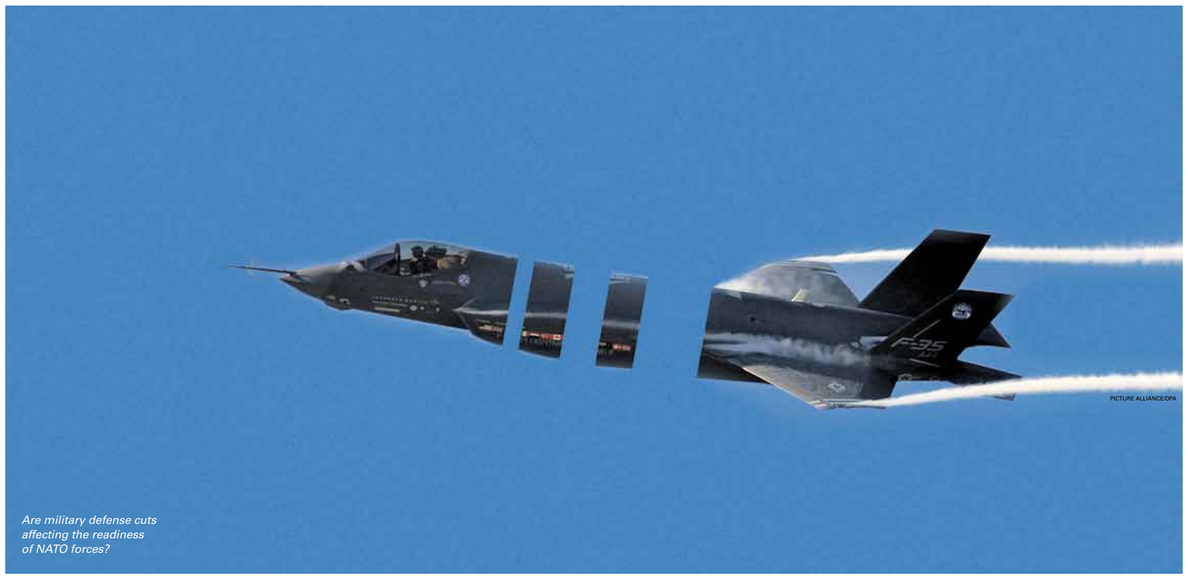
Of course this transformation comes at a risk: Al-Qaeda is lacking coherence and leadership. In almost every theater there are severe internal conflicts. AQIM has splintered; al-Shabaab assassinates dissident cadres; in Syria al-Qaeda is present with two groups at the same time, one loyal to al-Zawahiri, the other to the AQIM leadership.

All of this has weakened al-Qaeda. The organization is not in good shape – as an organization. But what could be called the global Jihadist movement – with al-Qaeda at its helm – is faring well. The net result is as troubling as it is evident: Al-Qaeda and its allies are as big a threat to global security as they have ever been. ■

Yassin Musharbash is a Berlin-based investigative reporter and terrorism analyst with the German weekly newspaper Die Zeit.

ANNIKA LANGOSCH

Flashpoint AL-QAEDA



PICTURE ALLIANCE/DPA

Are military defense cuts affecting the readiness of NATO forces?

Don't underestimate the West

Rising powers continue to increase defense spending but NATO forces remain powerful | By Alexander Nicoll

We all know today's headline about defense: the United States and Europe are in headlong decline, and the new big spenders are Asia's rising powers. On one level, the story is correct. The extent of reductions in the Pentagon's budget may end up greater even than those mandated under congressional sequestration, and Asia is now spending more than Europe on its militaries. But all such assessments depend on the timeframe. If we consider the period since the Cold War as a whole, the budget picture is less dramatic.

In the twenty years after 1990, spending on defense by NATO members rose 27 percent in real, inflation-adjusted terms, according to NATO figures. Of course, 12 nations were added to the Alliance during that time, but these all have relatively small defense budgets. The biggest factor in the increase was the doubling in the amount spent by the United States in the decade following the 2001 terrorist attacks on New York and Washington. It is not surprising that, with the war in Iraq over and foreign forces withdrawing from Afghanistan, the figure is now subsiding.

The amount spent on defense is just one measure: what matters is how you spend the money. In terms of capabilities, the change is perhaps more dramatic than is often portrayed, and should give the world's rising powers pause for thought. Because of constant involvement in operations – in the Gulf, the Balkans, Iraq, Afghanistan and elsewhere – the West's armed forces have been forced to transform themselves, leaving behind the more static postures of the Cold War.

The change is not as all encompassing as that forecast by advocates of the 1990s 'Revolution in Military Affairs', in which new technologies were seen as offering command of a 'battlespace.' That vision proved unrealistic. But today's Western armed forces instead use new military and commercial technologies in innovative ways to help them deal with real-world battlefield threats. They have been taught hard lessons, and the degree to which painful operational experience has influenced them should not be underestimated. They may not have 'won' the wars in Iraq and Afghanistan, but they have learned a lot from them. As a result, the West's armed forces may in future be smaller, but they will still be potent.

Trends in defense spending since the fall of the Berlin Wall have had several drivers. First, there was the post-Cold War peace dividend. According to NATO figures, US defense spending fell 24 percent in real terms between 1990 and 2000, and spending by NATO's European members fell 10 percent in the same period. As a proportion of gross domestic product (GDP), American spending dropped from 4.4 percent in the first half of the 1990s to 3.2 percent in the second half, and NATO Europe's from 2.5 percent to 2.1 percent. The number of active personnel under arms in the United States dropped from 2.1 million in 1990 to 1.5m in 2000, and in NATO Europe from 3.5m to 3m.

The second factor was the 'war on terror' declared by President George W. Bush in response to the 9/11 attacks. This brought a divergence in trends on either side of the Atlantic, with America's defenses expanding rapidly and Europe's remaining essentially stable or in slow decline.

NATO figures show that American spending rose 100 percent in real terms between 2000 and 2010, while NATO Europe's fell just two percent in the same period. As a proportion of GDP, American defense spending averaged 3.4 percent in the first half of the decade and 4.5 percent in the second half, rising to a peak of 5.4 percent in 2010. The average in NATO Europe was 1.9 percent in the first half of the decade and 1.8 percent in the second. Active personnel under arms remained almost unchanged in the United States between 2000 and 2010 but fell in NATO Europe from three million to two million.

The third driver is the performance of economies and the related pressure on government budgets as a whole. The Great Recession that began in 2008 and the debt crisis afflicting Europe since 2009 have had an important effect on defense budgets. According to the Military Balance 2013, global defense spending fell in real terms by 1.5 percent in 2011 and two percent in 2012.

In the United States, the breakdown in Congressional politics meant that no agreement could be reached on how to cut discretionary spending, and so the Budget Control Act of 2011 mandated across-the-board cuts: a $487bn reduction from the president's 2011 defense budget request, spread over five years; and a further 'sequestration' of some $500bn over ten years from 2013 if no new fiscal legislation could be passed, which it was not.

PRIVATE

Alexander Nicoll is Senior Fellow for Geo-economics and Defense at the International Institute for Strategic Studies.

Flashpoint DEFENSE BUDGET

The full implications of these cuts are not yet known. A study commissioned by Secretary of Defense Chuck Hagel concluded that the Pentagon could either reduce the size of the defense establishment now and invest funds in future capabilities, or maintain present capabilities at the expense of investment in the future. The more likely outcome was somewhere in between these options.

However, some defense budget experts believe that Congress will continue to reduce defense budgets in future years and that the resulting level of spending will be even lower than that currently contemplated. If that is the case, some important equipment programs might have to be cancelled – but at present, this is not occurring. Indeed, the United States still has a very active acquisition program for new equipment and capabilities – such as the F-35 Lightning (Joint Strike Fighter) program – in spite of budget cuts.

The trends are different elsewhere. According to the Military Balance 2013, defense spending in NATO Europe fell in real terms by 2.6 percent in 2011 and 1.5 percent in 2012. In Asia, continuing rapid economic growth (even though slowing somewhat) has led defense spending higher, so that in 2012 in nominal terms it exceeded that of NATO Europe for the first time, with China accounting for a large part of the rise.

It is useful, however, to keep in mind that the United States is still by far the world's largest defense power, and is set to remain so for some time to come. Even at its reduced level of spending of $645 billion in 2012, it exceeded the next 14 countries combined. Though European armed forces bemoan the cuts that they have been forced to accept, they still pack a punch, and three European countries – the United Kingdom, France and Germany – continue to be among the world's top ten defense spenders, respectively third, seventh and eighth.

The key question will be how continuing cuts are implemented and what this will mean for the future capabilities on both sides of the Atlantic. Investments made in the past, when combined with operational experience, have produced significant advances.

In the 1990s, the big change was the arrival of precision weapons, considerably increasing the effectiveness of bombing campaigns and missile strikes. In the following decade, Western armed forces have combined these targeting abilities with networked surveillance and intelligence technologies so that air and maritime capabilities have become much more integrated with operations on the ground.

The time taken to identify a target and then strike it has shortened considerably. As budgets fall, unmanned systems can help to maintain this edge. In addition, the nature of the wars in Afghanistan and Iraq has provided substantial ground combat experience, including in difficult terrains. Militaries have had to adapt to enemy tactics such as the planting of improvised explosive devices.

It has to be kept in mind that in both wars, Western forces had complete command of the airspace. In a future conflict, this might not be the case. Also, neither campaign resulted in the defeat of the enemy on the battlefield.

Nevertheless, Western forces now possess a large amount of operational and collaborative combat experience, as well as retaining powerful air forces and navies. They are still investing in future capabilities. And initiatives now under way may enhance cooperation among European countries so that value for money from defense budgets is enhanced.

While rising powers will continue to increase defense spending as their economies expand, they will still lack the technological expertise and the experience possessed by Western nations. In spite of today's headlines, the West's ability to project and use military power will remain something to be reckoned with. ■

Discretion guaranteed

Germany provides a forum for talks as isolated North Korea seeks contact with the US | By Matthias Nass

Discretion was the top priority on Sept. 25 and 26, when delegations from two countries that aren't officially talking to each other gathered in a Berlin hotel. Diplomacy calls this kind of talks "track two." It's where you meet when you have nothing to say to each other at government level – like Americans and North Koreans.

They sat together for two days in a Mercure Group hotel. The diplomats who arrived from Pyongyang would normally play a prominent role in any official negotiations. They included Vice Minister of Foreign Affairs Ri Yong-ho and Choi Seon-hee, the Deputy Director General of the American Affairs Bureau.

The US delegation was led by two of the country's most experienced diplomats. Stephen W. Bosworth served as Special Representative for North Korea Policy and currently heads the US-Korea Institute at Johns Hopkins University. Robert Gallucci was the chief US negotiator during the North Korean nuclear crisis in 1994 and, after leaving government work, became the dean of Georgetown University's School of Foreign Service.

The Americans did not come as envoys of their government. They had taken the initiative themselves. The US State Department believes that anyone meeting with the North Koreans is naïve, one participant said. But it would be hard to find any ex-diplomats more experienced and free of illusions in dealing with dictatorships like North Korea than Bosworth and Gallucci, the source added.

In the US, where people and ideas circulate briskly between the government, think tanks and universities, it's often possible to make things happen without holding government office. That was the background to the meeting in Berlin.

A fair amount is currently at stake between Washington and Pyongyang. Only six months have passed since North Korea's young leader Kim Jong-un introduced martial law and threatened the US with a pre-emptive nuclear strike. Americans and North Koreans last sat together at a negotiating table in 2009, when Pyongyang broke off the six-party talks in Beijing over its nuclear arms program. A dangerous silence.

In Berlin, the Americans sought to gauge what kind of agreement would still be possible between the two states. For the time being the Obama administration sees little reason to engage with the North Koreans. Without clear indications that Pyongyang is willing to give up its nuclear weapons there are no grounds for official talks, the White House says.

The North Koreans brought a message from Pyongyang that North Korea was eager to return to the six-party talks, but without preconditions. That may be connected to reports that the North recently restarted its nuclear reactor at Yongbyon.

China, North Korea's sole remaining ally, recently increased the pressure on its small neighbor. Senior politicians all the way up to party chief Xi Jinping have warned the regime to drop its belligerent posturing and show willingness to negotiate. China also appears to be upholding the UN-imposed arms embargo on North Korea, at least in part.

Washington is more than willing to let Beijing bear the main burden in this conflict. The US is acting "disinterestedly" in regard to North Korea, a participant in the Berlin meeting said. That source pointed out a "New York channel" for talks, where North Korean UN representatives meet with junior US diplomats. Otherwise, the source said, it is the Chinese who transmit messages between the US and the North. "Our policy is not working," the source said. Asked whether a new round of six-party talks could be expected in the foreseeable future, the source answered, "I don't see that."

Flashpoint KOREAN PENINSULA

What a contrast to the rapprochement between the US and Iran! Barack Obama is engaging the new Iranian President Hassan Rouhani with open arms and investing much political capital in his bid to resolve the nuclear conflict with Tehran. In mid-October the UN Security Council's six veto powers plus Germany negotiated with the Iranians in Geneva. Toward Kim Jong-un, on the other hand, Obama is keeping an icy distance and ignoring the craving for recognition that Kim's father and grandfather likewise exhibited.

Nonetheless, Obama's Secretary of State John Kerry himself took part in a confidential meeting with North Koreans in New York in March 2012. At the time he was still chairman of the Senate Foreign Relations Committee. The meeting was organized by Germany's Friedrich Ebert Foundation. In the past, Berlin's Aspen Institute has also brought together representatives from the two states.

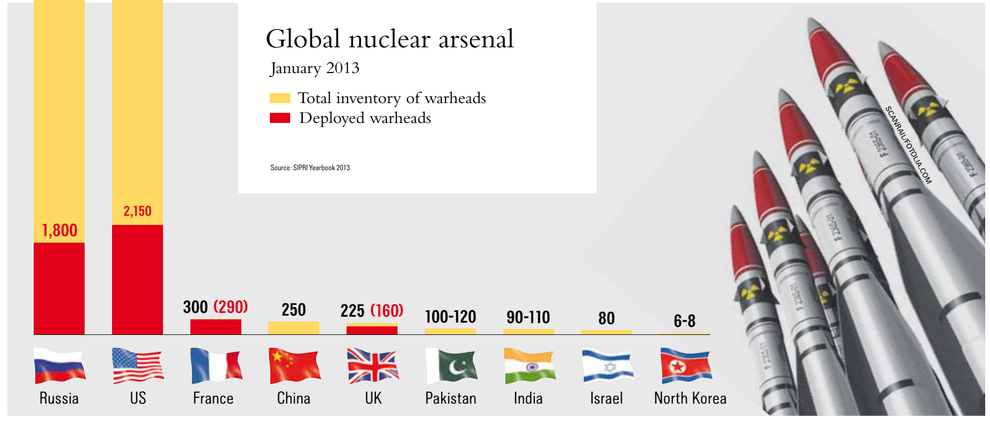
Why the Germans, one might ask. One big reason is that Berlin, unlike most other Western governments, maintains ties with Pyongyang through its own embassy there. That gives the Germans channels and contacts that other states do not have. Also, the Germans, themselves once a divided nation as Korea remains to this day, seek to encourage a dialogue there. Change through engagement worked for us, the Germans reason. Why not for Korea as well?

That's why Berlin will continue to help where it can – with the utmost discretion. ■

This article was originally published in Die Zeit on Oct. 17, 2013.

PICTURE ALLIANCE/AP PHOTO

This satellite image appears to show new construction at North Korea's Sohae missile launch site near the northern border with China.



Don't write off Assad

The West needs a new Syria strategy | By Michael Lüders

By now it's an old saw, but it still bears repeating: There are no simple solutions for Syria, now and probably for years to come. The fronts have become far too blurred and overlaid; too many actors are taking part in the country's (self-)destruction.

What began in March 2011 in the wake of the Arab Spring as a popular uprising, mostly within poorer sections of the Sunni Muslim majority, has long since evolved into a civil war along ethnic and sectarian fault lines. This civil war has moreover become pervaded by a proxy conflict in which, in simplified terms, two camps face each other.

The Western powers, especially the United States but also the Europeans, together with Turkey and the Gulf states, seek to topple Bashar al-Assad and his regime – not because he's a tyrant (the Gulf rulers are too) but because of the Tehran-Damascus-Hezbollah-Shi'ite axis. The Syrian regime is Iran's sole ally in the Arab world, its territory the pipeline for arms shipments to Hezbollah.

Assad's foes reckon that if his regime falls, Sunnis – who account for 60 percent of the country's population – will almost certainly take over in Damascus. It's hoped that they would turn to Riyadh and Washington for support and cut the privileged ties with Tehran. Hezbollah would be cut off from its arms supplier – which is why its fighters, experienced in house-to-house fighting, are actively supporting the Assad regime's struggle against the rebels.

Of course, that is also why Iran is backing Assad at all costs. The same goes for Russia and China, both trying to block a further expansion of the Western zone of influence in the Middle East, especially after what they witnessed in the Libyan intervention, when Washington, London and Paris used an explicitly limited UN resolution for intervention to overthrow the Gaddafi regime.

Both sides, Assad's friends and foes, are ruthlessly pursuing their own political and geo-strategic interests with no regard for the loss and suffering among the Syrian population. In a real sense, the Syrian people's uprising has been held hostage by wider interests, their revolt taken over by global politics. This is the tragedy of Syria. What began as a peaceful protest, forcibly suppressed by Assad's army and police, has become a struggle for sheer survival. For millions of people that has meant migration, expulsion, suffering and death, with no end in sight.

The Assad clan belongs to the Alawite minority, an offshoot of Shi'a Islam, which constitutes about 15 percent of the population and, since the 1970 seizure of power by Bashar al-Assad's father Hafez, has controlled the levers of power. To stabilize their power base the Alawite elite cut a deal with Sunni traders and businessmen early on: Make all the money you want so long as you accept that we are in charge.

In the wake of the revolt the regime has reinvented itself or, more precisely, learned to focus its force. Initially it attempted to take on the rebels everywhere in the country. Now it is concentrating its efforts on the Alawite heartland along the Mediterranean coastline as well as around Damascus and Homs. It has largely abandoned the northern and eastern territories, although these areas continue to be hit by air strikes and shelling. Syria's economic hub Aleppo, now mostly in ruins, is a divided city: The rebels hold one half, the army the other.

The deadlock in the country has also partly resulted from distorted assessments of conditions in Syria. Many people simply say: Assad is a butcher. He has to go, so that the opposition can start building a democratic Syria. Very early in the conflict, almost all Western governments broke off relations with Assad in the mistaken assumption that he would soon be toppled, just like Gaddafi.

Syria is not Libya, however. For starters, the "moderate opposition" figures so courted by Western governments represent practically no one but themselves. They have gathered into several groups, of which the best known is the Sunni-dominated "Syrian National Council" based in Istanbul, which recently also started calling itself the "Syrian National Coalition." Its leadership changes sometimes monthly, something that has no further consequences, however, because its decisions are ignored inside Syria. More and more rebels have cut their ties with it. It never had a command structure over the "Free Syrian Army" anyway.

Ultimately this is where the Syrian exiles have demonstrated their incapacity to act strategically. They have yet to establish an exile government, largely because they are caught within the same tribal state of mind as the Assad regime. Arabs can't work with Kurds, no Sunni would accept an Alawite to represent his interests and vice-versa, Muslim Brothers refuse to work with women or leftists and vice-versa. Add denial and an inability to self-criticize to the mix. At the urging of their benefactors in the West and the Gulf states, the Syrian exiles tend to put forward maximal demands, i.e. no negotiations with Assad.

Put simply, the West has bet on the wrong horse. The Russians, Chinese and Iranians knew from the start what they wanted. In Washington and elsewhere, meanwhile, we see hesitation and an endless stream of second thoughts. For good reason, one might add, as radical jihadists long ago began setting the agenda within the rebel camp. If we believe the intelligence report by military analysts IHS Jane's published on Sept. 14, the Syrian rebels number about 100,000 fighters, divided into about a thousand groups, splinter groups and gangs.

Definitely the strongest, the report says, are the jihadists. Some 10,000 are allied with al-Qaeda, namely the Nusra Front and the "Islamic State of Iraq and the Levant" (ISIL). Another 30,000 to 35,000 jihadists are fighting in Syria for a clerical state without an "international agenda." Moderate Islamists number another 30,000, while secular or purely nationalist groups such as the Free Syrian Army muster the fewest combatants.

In brief, the civil conflict is increasingly becoming a sectarian and ethnic war – as well as a proxy theater for the rivalries between Russia and the US, respectively the West, and between the Gulf States and Iran. Ironically, yet also tellingly, the Gulf monarchies, led by Saudi Arabia, bankroll many of the jihadi groups. Against this background the now-canceled intervention in Syria would have become a preposterous undertaking, seeking to topple Assad and help the jihadists take power in his wake.

Cynics openly advocate promoting a deadlocked conflict in which neither side gains an upper hand, believing that this would be in the best interests of the US and Israel. These voices accept rising instability in the entire region, not least due to the influx of millions of Syrian refugees in neighboring countries as a necessary price to pay.

Instead, pragmatism is what's needed now. The plan to destroy Syria's chemical arsenal under UN monitoring, drawn up almost incidentally, was a first step.

It is worth noting that some of these weapons have been stored in areas now controlled by rebels. One might question the assertion that they did not have the technical resources to mount the poison gas attack in a Damascus suburb in August that killed hundreds of civilians.

There must be a follow-up. The peace conference planned for November in Geneva must bring together the government and those rebels willing to negotiate – without regard for the sensibilities of Syrian exiles. US Secretary of State John Kerry has stressed that President Assad has no place in a transitional government. Given the recent successes of Assad's forces on the ground, he certainly has no reason to bow to Washington's wishful thinking. Assad will probably stay in power for the time being. He may soon become a sought-after ally in the fight against al-Qaeda, especially along the Turkish border. ■

Hello again? "Assad will probably stay in power for the time being. He might become a sought-after ally in the fight against al-Qaeda."

AFP/GETTY IMAGES

Iranian President Hassan Rouhani at the UN General Assembly in New York in September.

PICTURE ALLIANCE/ZUMA PRESS

Time to talk

Is Iran ready to come in from the cold?

By Matthias Nass

High hopes accompanied the opening of a new round of negotiations over Iran's nuclear program. The talks between the clerical regime and the five UN veto powers plus Germany began in mid-October in Geneva and are scheduled to continue early in November. They will show whether Tehran is serious. Or, more concretely, whether Iran's new President Hassan Rouhani, can negotiate a deal with the P5+1 that the supreme leader, Ayatollah Ali Khameini, will accept.

For decades, US-Iranian relations have been a narrative of missed opportunities. Sometimes it was the conservatives in Washington who did the stonewalling, other times it was the hardliners in Tehran. This time the outlook seems brighter.

For weeks Rouhani had communicated that he was prepared to resolve the long-standing concerns about Iran's nuclear ambitions. And so far, Ayatollah Khamenei is backing his president. He has even instructed the Revolutionary Guards, who set much of the foreign policy agenda under Rouhani's predecessor Mahmoud Ahmadinejad, to stay out of politics.

Tehran's change of tack is down to more than the new president's wisdom. Iran is suffering under a regime of punitive international sanctions imposed specifically in response to the government's intransigence on the nuclear issue. The already fragile economy contracted 6 percent last year. Oil production fell by more than half within a year. The inflation rate hovers at about 60 percent; unemployment at 30 percent. Iran's currency, the rial, has lost over half its value in the past 20 months.

In the White House too, the mood has changed. During the recent session of the UN General Assembly, Barack Obama and Rouhani made the first direct contact between the United States and Iran in more than three decades. While they did not meet in person, the two leaders spoke on the telephone.

Obama said goodbye in Farsi: "Khodahafez," – or: God be with you. With these words the US president wished his Iranian counterpart a good flight back to Tehran from New York's Kennedy Airport, where Rouhani was headed when Obama called.

God be with you? What's gotten into the "Great Satan" America? In fact, a great deal is in flux these days. Suddenly, time-honored prejudices and worldviews no longer ring true. The phone call between Obama and Rouhani lasted only 15 minutes, but those minutes ended 34 years of official silence between Tehran and Washington.

Is this another Nixon-in-China moment? A diplomatic breakthrough of the magnitude of the then US president's visit with Mao Zedong in 1972?

The Iranians want to emerge from their isolation. On this point there really are parallels between Beijing in 1972 and Tehran in 2013. After the maelstrom of the Cultural Revolution China was isolated internationally, with a ruined economy and bankrupt ideology. A great civilization had slammed shut the gates to the outside world and all but consumed itself in a spasm of messianic fervor and state terror.

There is no permanent revolution. No nation can endure that. As China did, so Iran must today find an exit from its self-inflicted decline. Rouhani promised as much to his people, and that was why they voted for him. Now, at the second round of nuclear talks in Geneva, the Iranian side will have to demonstrate its commitment. Apparently, it has already made a promising start.

In Geneva, Iran's Foreign Minister Mohammad Javad Zarif set out Tehran's proposals in an hour-long Power Point presentation entitled "Closing an Unnecessary Crisis, Opening New Horizons." He gave his presentation in English. The ensuing discussions, described by a senior US official as "intense, detailed, straightforward and candid," were also – an absolute novelty – conducted in English.

There was no breakthrough in Geneva, but the mood on both sides was surprisingly buoyant. Catherine Ashton, the EU foreign policy chief who chairs the six-nation group, called the talks "substantive and forward-looking," Zarif said the meetings had been "fruitful." Of course, none of this means that getting a deal will be easy.

The details of the Iranian three-part plan have only sketchily seeped into the public domain. In the first stage, so it seems, Iran and the six powers would outline the contours of a confidence-building process, with Iran constraining part of its nuclear program, the US and the EU reining in their sanctions regime.

In the second stage, the "end state" would have to be defined – the extent to which Iran would be permitted to continue its nuclear enrichment program. This would certainly entail a Western assurance that Iran could retain a limited right to enrich uranium, as well as Iranian acceptance of strict and intrusive inspections. The third stage of what the Iranians consider as a six-to-twelve-month process would finalize the restrictions regime and terminate Western sanctions.

Shortly before the first Geneva meeting, Hossein Mousavian, Iran's ambassador to Germany in the nineties and a close collaborator of Rouhani, gave a talk at the Körber Foundation in Hamburg. It shed some additional light on what the Iranians are after.

If all goes well, the two sides could agree on four principles in Geneva, Mousavian said. The Iranian side would have to make two pledges. First, Tehran would agree to full transparency, i.e. allowing the Vienna-based International Atomic Energy Agency (IAEA) to make unannounced monitoring checks on all Iran's nuclear facilities. Second, Tehran would commit itself to enacting confidence-building measures that would hinder Iran from using its nuclear program to build bombs. That would lay to rest the fears of Western governments that the civilian nuclear program might serve as a platform for producing nuclear weapons.

In return, the P5+1 would have to acknowledge Iran's fundamental right to enrich uranium and use nuclear energy peacefully. As a signatory of the Nuclear non-Proliferation Treaty, Iran enjoys this right in any case. Finally, the world powers would declare readiness to lift the sanctions.

Once unity is reached on these four principles, the details could be worked out, Mousavian said. Echoing Rouhani, he expressed optimism. The negotiations could be wrapped up within six months, he said, adding: "That's enough time."

There is widespread agreement about what a deal could look like: Iran would enrich its uranium to not more than 5 percent: enough to run a nuclear reactor but insufficient for a nuclear weapon. Its stocks of 20 percent enriched uranium would be handed over. The Fordo enrichment site, located deep inside a mountain and secured against military strikes, would be decommissioned, as would the soon-to-be-completed heavy water reactor at Arak, which could also produce plutonium. Iran would submit to unrestricted monitoring of all its nuclear facilities by the IAEA. But the country could produce nuclear energy and the sanctions would be dismantled step by step.

The question is of course: Can Iran, can the West overcome habitual distrust to close the deal? Ever since the US embassy in Tehran was seized for 444 days in 1979, the US and Iran have been locked in a relentless confrontation, vilifying each other as the "Great Satan" or a "rogue state." Now for the first time in 34 years, detente between them seems no longer unimaginable – provided that cool heads prevail.

"The real question is whether hardliners in both Tehran and Washington sabotage whatever comes out of this effort to resolve the nuclear issue and improve US-Iran relations," as Ryan Crocker, a veteran of US diplomacy in the Middle East, put it in Time Magazine.

Hardliners on both sides are already up in arms. In Tehran, the commander of the Revolutionary Guards, Mohammad Ali Jafari, called the phone conversation between Rouhani and Obama "a tactical error," while in the US congressional hawks are calling for further sanctions. They would leave all existing sanctions in place even if Iran gave up its uranium enrichment completely.

The diehards on the Hill worry that any peaceful program would inherently lead to a military program, allowing Iran suddenly to break free sometime in the future. According to some estimates, with close to 20,000 centrifuges, Iran is already able to produce enough weapons-grade uranium for a single bomb in just six weeks.

Such scenarios explain why zero enrichment is also the demand of Israel's Prime Minister Binyamin Netanyahu. He has matched Rouhani's charm offensive with a hardline media blitz of his own.

However, complete disarmament and total demolition is not a realistic outcome. Iran would have to accept invasive monitoring and complete transparency. If the Iranians don't follow through, there will be no deal and the crippling sanctions will remain in place.

A less belligerent relationship between Tehran and Washington, bolstered by a resolution of the toxic and seemingly intractable nuclear question, could transform the Middle East. Rouhani's position would also be buttressed if a deal could be reached. Then, after the eight dismal years under Ahmadinejad, a cautious liberalization within Iran could also become possible. That, too, is at stake in Geneva.

Securing a deal is tough enough as it is. It would be foolhardy to needlessly complicate an already complicated situation by imposing even harsher sanctions on Iran. Europe must try to prevent this. ■

Matthias Nass is International Correspondent for the German weekly Die Zeit.

W. BARTSCH

Flashpoint IRAN

Michael Lüders is a political scientist and Islamic studies scholar.

PRIVATE

Flashpoint SYRIA

An active Alliance in a globalised world

The Afghanistan mission is not NATO's swan song, it testifies to the alliance's political cohesion and military stamina

By Michael Rühle

What will become of NATO after Afghanistan? Will an alliance without a major ongoing military operation lose its relevance? Will operational fatigue lead Allies to lower their military ambitions?

Such are the questions that dominate the current debate about NATO's future. Yet these are moot questions. True, NATO's leadership of ISAF (International Security Assistance Force) defined the organization in many ways: it shaped NATO's political and military outlook as well as its relations with other countries and institutions. Moreover, NATO will not escape a debate over whether the mission was ultimately "worth it."

Yet NATO can face this debate with confidence. No other organization worldwide could have sustained such a complex mission at such great distance over such a long period of time. And only NATO could have brought so many partner countries into this common endeavor. Hence, far from being NATO's swan song, the Afghanistan mission testifies to NATO's political cohesion and military stamina.

The end of ISAF is simply the end of one unique chapter in NATO's evolution. Another chapter has already started, quite different from the previous one but hardly less difficult to write: enabling NATO to respond to the post-Afghanistan strategic environment. This environment is characterized by three major transformations, each of which will confront NATO with new challenges: the globalization of security risks, the US pivot to the Asia-Pacific region, and the financial crisis.

The globalization of security risks manifests itself in failing states, the proliferation of weapons of mass destruction, new energy vulnerabilities, and the rapidly growing number of cyber attacks. All these risks do not correspond to traditional military patterns, but they will be serious enough to keep national security establishments fully mobilized.

These risks challenge Alliance solidarity, since they may not affect all Allies in the same way. And they challenge NATO's importance among the family of global institutions, since military responses will not always be appropriate or the first line of defense.

The US pivot to the Asia-Pacific region, in turn, diminishes Europe's role in the US security calculus. At the same time, it begs the question as to a common transatlantic approach vis-à-vis a region that Europeans thus far have been reluctant to view as being more than just an economic opportunity. Finally, the financial crisis will curtail Western defense budgets for the foreseeable future, thus further complicating collective Allied responses to new challenges.

All these developments run counter to NATO's traditional political and military mechanisms. The challenge, then, is to adapt NATO so as to avoid the loss of relevance that failure to tackle these developments effectively will inevitably cause. This adaptation must proceed on three levels: political, military and institutional.

On the political level NATO must deal more systematically with longer-term security developments. The reflex of only wanting to discuss issues of immediate military relevance runs the risk of being overwhelmed by the multitude of globalisation's challenges.

To mention but one example: An alliance that discusses the implications of a nuclear armed Iran only once concerned Middle Eastern partner countries put it on the agenda, has not yet truly arrived in the 21st century. At the same time, NATO must continue to enable the formation of flexible coalitions within the alliance, albeit supported by the NATO command structure. This will ensure that a group of likeminded allies (and partner nations) will act even if other allies do not, as was the case in the 2011 Libya operation. Since many new challenges will not affect allies in quite the same way, flexible coalitions are the appropriate means to prevent paralysis.

On the military level, the Alliance must remain focused on expeditionary forces for contingencies beyond NATO's borders. This follows from the nature of globalized challenges, which need to be addressed at their source. It also follows from the need to be able to act together with the US. For NATO to succumb to the temptation of "coming home," i.e. to re-focus on territorial defense, would be a strategic regression, as it would decouple NATO from the security agenda of the United States. A reorientation of NATO away from its expeditionary character would send a signal to Washington not to count on European support in non-European crises. This could herald the de facto, if not de jure, end of NATO. The need to act alongside the US also requires enhancing NATO's exercises regime in order to ensure the continued interoperability of allied forces in a period without major operational commitments.

On the institutional level, NATO must continue to deepen its partnership network with partner countries, including with those from the Asia-Pacific region. A NATO-led operation without the involvement of partner countries has become almost inconceivable. Partners not only provide all kinds of military support, which is crucial in times of budgetary austerity, but also enhance the legitimacy of a mission. It is therefore essential that NATO's cooperation with partners, which used to be catalyzed by the Afghanistan deployment, will remain vibrant even after 2014.

At the same time, NATO must deepen its cooperation with other international institutions and NGOs, as such cooperation will be the key to making a "Comprehensive Approach" to crisis management work. NATO must also enhance its ties with the scientific community in order to understand the security implications of climate change or the global competition for energy and other resources. The same holds true for partnerships with the private sector: the latter's expertise on cyber defense and energy security, for example, may turn out to be crucial for NATO's own efforts in this area.

Will the allies be ready to meet the challenge of reform? Up to now, this question remains unanswered. In 2010 allies agreed on a Strategic Concept that offers a cogent description of a modern alliance ready and able to cope with globalization's challenges. Yet the financial squeeze, as well as a certain amount of Afghanistan fatigue, are powerful countervailing forces that might lead some allies to opt for a more modest, eurocentric NATO.

So when NATO's Heads of State and Government meet in 2014 in the United Kingdom for their next summit, they would do well to reaffirm their commitment to modernize the alliance along the lines envisaged by the Strategic Concept. Such a reaffirmation would be a fitting complement to the end of ISAF, as it would demonstrate that even after Afghanistan NATO will remain an active alliance in a globalized world – and project stability even if it is not always projecting force. ■

Michael Rühle is Head of the Policy Planning and Speechwriting Section for NATO's Political Affairs and Security Policy Division.

PRIVATE

Flashpoint AFGHANISTAN

Pacific hegemon

China continues to expand its military capacity and operational range in disputed waters

By Isabel Hilton

The Liaoning aircraft carrier is a clear signal of China's intentions in the Asia-Pacific.

PICTURE ALLIANCE/DPA

In September 2013, nearly a year after it was formally commissioned into the Chinese navy, the refurbished Soviet-era carrier that the Chinese had re-named the Liaoning completed a sea trial that included testing the capacity of its pilots and planes to take off from, and land on, what is China's first and only aircraft carrier. The trials were pronounced a success, a signal no doubt of China's intention to enlarge its embryonic carrier fleet.

The Liaoning, as Chinese media readily admitted, is approximately three decades behind the latest US carrier, the nuclear-powered USS Gerald R. Ford, launched in October 2013 and slated to be the most advanced vessel in the US Navy. Despite boasting the largest naval force in Asia, China's naval capacity remains underpowered in comparison to both the US and Japan. As of the end of 2012, according to US estimates, the Chinese navy comprised around 79 principal surface warships, more than 55 submarines, 55 medium and large amphibious ships, and roughly 85 missile-equipped small ships.

If the US fulfills its announced intention to deploy 60 percent of its naval power in the Pacific by 2020, China would be heavily outgunned. But the interest that the progress of the Liaoning aroused in China's neighbors derives not from any claim, or intention, to match US firepower, but from concerns about the creeping success of China's low key aggression in the disputed waters of the South and East China Seas.

In addition to the Liaoning, China has boosted investment in advanced short- and medium-range conventional ballistic missiles, land-attack and anti-ship cruise missiles, counter-space weapons, and military cyberspace capabilities designed to enable area-denial, according to the US annual report to Congress on China's military. It has also improved nuclear deterrence and long-range conventional strike capabilities; advanced fighter aircraft; limited regional power projection and undersea warfare.

Preparing to retake Taiwan is still the headline objective of this investment, though China's capacity to launch an amphibious assault on the scale required remains distant, and China remains politically committed to a peaceful reunification. China's more immediate military interests include counter-piracy, peacekeeping, disaster relief, and regional military operations, of which the territorial disputes in the South and East China seas are the most prominent.

Here, despite its nominally superior strength, the United States has proved powerless to counter Chinese territorial creep. In 2006, the then US secretary of State Hillary Clinton declared that the free passage of shipping in the South China Sea was a US vital national interest, but the US Mutual Defense Treaties in the Asia-Pacific do not commit the US to get involved in territorial disputes in which it has no claim.

China's signals meanwhile, are characteristically ambiguous: whilst warning the United States not to interfere, China has also said that it intends to join the 22-nation Rim of the Pacific naval drill, led by US Forces, in 2014. While reassuring the world that it does not seek hegemony, China continues to expand its military capacity and the range of its operations.

When, in December 2012, China attached to its passports a map that claimed almost all of the South China Sea (along with the Indian state of Arunachal Pradesh) as Chinese territory, China's neighbors were in the awkward position of accepting the passports, which might imply acceptance of the claim, or refusing them and risking economic and political retaliation. It was a move characteristic of China's approach to the mosaic of competing claims over the rich oil, gas and fishing resources of the South China Sea.

The Spratly Islands are scattered over roughly 160,000 square miles of the coastal waters of the Philippines, Malaysia, Brunei, Vietnam, Taiwan and China, all of whom claim part of the islands and exercise effective control over several. The Paracel Islands are effectively under Chinese control.

China's naval behavior in the region has grown steadily more assertive in the last three years, not through the deployment of major naval firepower, but using a large fleet of smaller coastguard vessels, marine patrol boats and even fishing boats, that maintain a constant and creeping pressure on rival claimants' naval patrols, fishing fleets and other civilian vessels. It is a strategy that has allowed China to avoid direct military confrontation, while gaining territory through a series of soft confrontations.

In one such case, Beijing has gained effective control of Scarborough Shoal, known to China as Huangyan Island, where China and the Philippines had been in direct confrontation. When the US brokered an agreement for both sides' ships to leave in 2012, China stayed and has since denied access to the Philippines, claiming that its sovereignty over Scarborough Shoal is undisputed.

With few naval assets of its own, the Philippines is pursuing a legal case against China under the UN Convention of the Law of the Sea (1994), which both

Isabel Hilton is a London based writer and broadcaster. She is founder and editor of www.chinadialogue.net.

BBC

Flashpoint CHINA

parties have signed. But in another move that provoked protests from both Vietnam and the Philippines in 2012, the Chinese government declared that the recently founded town of Sansha, on Woody Island in the Paracels, was henceforth a prefectural level city that would administer the "Chinese" territories of the Spratlys, the Paracels, and Macclesfield Bank, or, as China names them, the Nansha, Xisha, and Zhongsha islands and their surrounding waters. The move creates the appearance of Chinese legal jurisdiction and serves to probe international reaction to its territorial expansion.

China's supporting tactics carefully avoid crossing any military threshold, using superior numbers of small ships to obstruct, or to threaten to ram, rival vessels. If the other party fails to react, it risks losing territory; if it retaliates with force, China could feel entitled to respond, claiming the right of defense against aggression.

In October this year, President Xi Jinping, taking advantage of US President Barack Obama's absence from the ASEAN summit, signaled his expectation that trade between China and ASEAN would reach $1 trillion by 2020. That prospect gives China more than enough clout to intimidate smaller neighbors over territorial claims. President Xi told the Indonesian parliament in the course of his trip: "We should abandon the cold war mentality, and cooperate to build security and jointly safeguard regional peace and stability."

The message was received with nervous skepticism by some of China's regional neighbors, sensitive not only to the behavior of China's naval patrols, but to such reported remarks as those of PLA Major General Luo Yuan's suggestion that the Diaoyu (Senkaku) Islands should be declared a Chinese military target range, or that of Rear Admiral Zhang Zhaozhong, who called for a blockade of Philippine outposts in the Spratly Islands. Neither view represents government policy, but such remarks serve to darken the mood music and do little to reassure rival claimants.

A different, but equally troubling dynamic operates in the East China Sea, where China continues to react strongly to the Japanese government's purchase of three of the five islets in the Senkaku (Diaoyu) group from private Japanese owners in September 2012. China has since regularly sent maritime law enforcement ships and aircraft to patrol within 12 miles of the islands. Although a less complex dispute than those of the South China Sea, China's confrontation with Japan is more sensitive, given the role that Japan plays in China's nationalist narrative, which makes Chinese concessions politically unthinkable. China is concerned about Japan's increasing military budgets and the possibility that Prime Minister Abe might succeed in revising Japan's pacifist constitution. The US has a more direct involvement through its base on Okinawa, close to the disputed islands, and China has repeatedly urged the US not to "encourage" Japan's claims.

Other than China's immediate territorial disputes, Chinese security concerns have grown along with China's lengthening supply lines and its growing investment in fixed assets beyond sovereign territory. In energy supplies alone, China is dependent not only on free passage of shipping through the Malacca Straits, but also on pipelines such as the Shwe oil and gas pipeline through Myanmar, which runs through troubled Kachin territory and is potentially vulnerable to Myanmar's volatile domestic politics.

Further afield, China remains dependent on the US security umbrella, for instance in the Middle East, the source of 40 percent of China's oil and a region in which it has virtually no strategic reach. As long as this remains the case, China is highly unlikely to seek an active military confrontation. So far, given the success of its asymmetrical approach, it has not needed to. ■

It's the energy economy, stupid!

The shale gas story is all about competitive advantage and strategic gains | By Kirsten Westphal

We have never seen energy markets like this before. Three dominant structural trends have been observed since the turn of the century: first, the steep demand increase in Asia, second, the still widely neglected fast growing domestic hunger for energy in the Middle East and North Africa, and finally, the fracking revolution making the US the world's largest producer of gas and oil.

The widening resource basis is a global phenomenon: larger shale resources in China and Argentina, Eastern Mediterranean offshore and East African gas discoveries, deep water and Arctic hydrocarbons. Whether these resources are being tapped and extracted depends on the combination of price developments, demand trends and technological progress.

Producers and consumers face enormous uncertainties about what the future global energy map is going to look like. While major European consumers as well as China and India have to prepare for increasing import dependency, the United States is bucking the global energy trend, with the prospect of becoming largely independent of fossil fuel imports.

America might even become an energy exporter, cutting into traditional suppliers' market shares. It will profit from comparatively lower gas prices in the years to come, which will give a remarkable advantage in terms of international economic competitiveness.

This will shape US foreign and security policy, providing Washington with a wider range of policy options as dependency on Organization of the Petroleum Exporting Countries (OPEC) diminishes. However, it is hard to imagine the United States ditching the Carter Doctrine (stating that the US will use military force to defend its national interests in the region) and withdrawing from the Persian Gulf and watching arms akimbo as other powers fill the vacuum in this strategic world region. But an end to import dependency will make it more difficult for Washington to maintain US public support for its role as global policeman.

Developments in the energy world are amplifying geopolitical processes that are already under way. Obama's Asian Pivot has gained political and economic momentum from the shale revolution, as energy trade diverts from the Atlantic Basin to the Pacific and sea lanes such as the Strait of Hormuz and the Strait of Malacca gain increased importance for Japan and South Korea. They are both close partners of the US, but they are also vital to China's energy supply.

The fear of a blockade of these vital seaways runs deep in all three. The pivot could be seen as constraining and countering China's rise, but also as a logical response to shifting trade flows. Russia is enhancing its military activities in the region, too and is also eagerly watching its Arctic backyard.

The shale revolution has hit the Arab world at a politically highly precarious juncture. Population growth and unemployment have fuelled protest.

Energy price subsidies have been one way to calm the domestic situation and to diversify the economy, but these policies bloat state budgets.

In future, moreover, rising domestic energy demand will lead the Arab world to consume a large proportion of its own energy, putting ever-higher financial pressure on states in the region. It is not only the resource rent strategies that are being called into question, but the very politics of generating affluence and securing power.

Kirsten Westphal is senior energy analyst at the German Institute for International and Security Affairs (SWP) in Berlin.

SWP

Flashpoint OIL & GAS

The political upheavals in the Arab world illustrate the geopolitical risks to which the global oil and gas sector is exposed, as the region remains the backbone of the global energy supply.

The perception of a relaxed hydrocarbons future is overhasty. If global demand continues as it is forecasted, it will have to be largely met by nonconventional resources and from the Gulf region. Energy markets tend to be cyclical and volatile in general, which means stress to the energy world. The OPEC members Saudi Arabia, Iran and Iraq will have to seek a sensible balance of interests. That adds tinder to an already incendiary regional situation. How will both Saudi Arabia and Iran align to China, already their number one customer?

Russia, formerly an indispensable energy power, faces marginalization and degradation into a swing supplier. This could reinforce its decline to mere regional power status. The Russian oil and gas companies are speeding up their diversification, particularly by aquiring market shares in China and the Asia-Pacific region. Russian liquified natural gas (LNG) is only one source in the Pacific, competing with Australian, Qatari and US LNG in the future.

Changing market power has geopolitical repercussions. This is equally true for Europe. It has profited from gas price pressure on its traditional suppliers, but it does not automatically follow that the US shale boom will result in more liquidity or more diversified supply. In fact, the shale revolution may increase instability in the neighbourhood as pressure mounts on the ruling elites of energy supplying nations. Europe must prepare for a regional contraction of its energy trade as well as for possible quantitative shortages.

As long as the three-way division of international gas market persists, with its accompanying price differentials, a scaled up "Atlantic Gas Corridor" is unlikely to materialize. Even though the gas price in continental Europe is three times higher than in the US, the real demand is in the Pacific market where risk premiums result in a 45 to 60 percent higher average LNG price than in the EU.

For Europe, Russia, the Caspian Basin, the Mediterranean and West Africa will be the primary regions to focus on. This is both a foreign policy but also an energy policy challenge. Connecting energy producers to Europe, open and functioning energy corridors with Turkey and Ukraine, enhancing energy cooperation and integrating markets are immediate strategic imperatives.

In the past Europe benefited from US guarantees of safe sea lanes and from initiatives to link the landlocked Caspian hydrocarbons to world markets. In the future Europe will have to fend for itself. Increasingly it is already competing directly with China in the Caspian and Central Asian regions, as well as in Russia. Its relative market share is going to decrease. This will jeopardize its supply security. That makes it all the more necessary that the EU bundles its forces in the global market and transforms its energy system.

In this situation, getting energy policies right is key. Shale gives us more time to transform our energy system, but does not obviate the need to do so. Fossil fuels yield short-term cost advantages but obstruct strategic decisions for a more sustainable energy future. At the same time, energy efficiency and renewables are important to hedge against resource conflicts and to provide greater energy security.

The trilemma of securing energy supply, protecting the climate and alleviating energy poverty will not be solved by the shale revolution. Shale oil, however, does not benefit climate security. While the US shale boom has served domestically to replace climate-damaging coal with gas, internationally coal is king.

The energy world is becoming more fragmented. Multilateral initiatives to shape energy relations are hampered by widely divergent interests. So what needs to be done?

Internationally, trust in markets and free trade must be strengthened. The US has to ensure confidence, as it is in the strategic position to make or break a global LNG market by approving hydrocarbon exports. The new times call for greater dialogue between producers and consumers and for a new integrated concept of energy and climate security. Collective approaches to maritime safety could help to reduce the risk of geopolitical friction caused by energy resource rivalry. ■

German fracking debate

Almost one in two Germans considers fracking an option to extract gas in Germany, according to a survey by polling institute forsa. But 90 percent of supporters believe it should only be allowed under extremely strict environmental constraints. Reducing energy costs for businesses was the most important argument for most of those in favor.

Unsurprisingly, German industry also finds this argument convincing. Chemicals major BASF is building a new ammoniac plant in the USA because the energy prices there are lower than in Germany. But CEO Kurt Bock also wants to exploit Germany's shale reserves. Speaking to the International Club of Frankfurt Economic Journalists, Bock called for test drilling to begin in Germany, saying this was the only way to show that fracking is safe and sustainable. "We would like to prove that," Bock said.

Cross party opposition in the Bundestag defeated a proposed law regulating the extraction of shale gas this summer. Germany's scientific community is also skeptical about fracking. The Hamburg Global Economic Institute (HWWI) warned against environmental damage and groundwater pollution. "As a country with a high-density population, Germany should not take a leading role in fracking," said institute director Michael Bräuninger. ■

The uses of intelligence

Has the expansion of America's surveillance technologies outstripped common sense? | By David E. Sanger

Step inside the giant glass cube that is the headquarters of the National Security Agency deep inside Fort Meade, halfway between Washington and Baltimore, and it does not take long before the leaders of what was once the most secretive intelligence agency in America start talking about the damage done by Edward J. Snowden.

"Tremendous harm, and ongoing," argues General Keith B. Alexander, during a recent discussion inside his office on the agency's top floor, overlooking a campus of domed antennas, which have sprouted with the expansion of the NSA's mission over the past decades. For all its focus on maintaining secrecy about how it cracks codes and – more recently – develops and deploys a new generation of cyberweapons, General Alexander and his aides have told Congress in recent months they never sufficiently appreciated the damage that could be wrought by an insider who violated his oaths to protect the nation's secrets and purposely undertook to expose the agency's operations.

Yet General Alexander's view is at sharp odds with the views of the 55 percent of Americans who told the Quinnipiac poll over the summer they view Snowden as more akin to a whistleblower than a traitor. When pressed, people who take that view often add that they do not doubt he did damage to American diplomacy, and to the NSA's ability to track terrorists. But even those who dispute the poll's findings concede that Snowden tapped into an abiding national suspicion that the expansion in the NSA's powers has come without debating the proper limits of government surveillance over the past dozen years since Sep. 11. And even President Obama – reluctantly – has said that it is "an important discussion to have," though one he clearly did not volunteer to begin himself.

Perhaps the biggest surprise is that the debate has been fueled by some of those who enabled the NSA to expand its operations. One of General Alexander's biggest challengers these days is a conservative Republican who was one of the authors of the Patriot Act, Congressman James Sensenbrenner. "We need to change the law and we need to change the law quickly," Sensenbrenner said in October, declaring it was time to put a stop to the NSA's bulk collection of "metadata" – the giant haystack of information about telephone calls, text messages and some computer traffic that has become the NSA's most critical database. A vote to stop funding on that program nearly passed the House of Representatives this summer. Sensenbrenner has also suggested that General James Clapper, the director of national intelligence, should be fired, or perhaps prosecuted, for publicly misleading Congress when he was asked whether American intelligence agencies routinely gather data on Americans. He said no, before the Snowden documents proved him wrong. (Clapper has apologized for giving what he called "the least untruthful" answer to that question; it seems clear that, at best, he was deliberately misleading.)

The Snowden revelations are unlikely to let up: He copied 50,000 or more documents, and more leak out every few weeks. The most recent revelations about how the NSA swept up millions of records of French phone calls and text messages, and how it tapped into the Mexican leadership, or the cellphone of German Chancellor Angela Merkel are only the latest in the steady trickle. Each major breach forces President Obama to call his counterparts with a half-apology, and a promise to re-evaluate. (In the case of France, the country's outrage was tempered a bit by the fact that French intelligence services are not shy about collecting on the US.)

And soon, the rethinking of the NSA's role is bound to accelerate. General Alexander has said he will retire early in 2014. When President Obama nominates his successor, the confirmation process in the Senate will become the centerpiece of the arguments over whether the astounding expansion of America's surveillance technologies has outpaced common sense. That is, essentially, the question the President has charged a small group of outside advisers to investigate. And while the group will not report back formally until the end of the year, the betting of insiders is that the NSA will not like all of the answers.

"What Obama wants to know is the answer to the question: 'Just because we can do it, should we?'" said one official familiar with the President's instructions to the group. "That's a very different question than 'Is it legal?'"

> "The Snowden disclosures have sewn so much distrust that they threaten to undermine President Obama's cyber protection agenda."

Experience suggests that President Obama will be reluctant to order major changes; as General Alexander often notes, "it isn't an accident" that only a handful of Americans have been killed by foreign terrorists since the Sep. 11 attacks. No American president, Democrat or Republican, wants to dismantle intelligence-gathering programs and then be blamed if another major attack occurs. The failure to detect or effectively respond to the attacks in Benghazi in 2012 that killed the American ambassador and three CIA employees left a lot of scar tissue on administration officials.

But based on conversations inside the intelligence agencies, with members of Congress, and with recently departed administration officials, a few early conclusions seem clear:

- Like other intelligence agencies, the NSA is going to be forced to think about the diplomatic consequences of its operations.

At the CIA, covert operations are reviewed annually. During that review, one standard question is "If this operation became public tomorrow, what would the diplomatic consequences be?" Yet astoundingly, the NSA's programs do not appear to be subject to the same kind of regular scrutiny. Until Snowden, its operations were rarely revealed to the public. And it's old, traditional role, the breaking of foreign codes, was not as sensitive.

But that has all changed – faster than the agency's top officials want to admit. The revelation that the agency was searching the metadata of millions of French telephone calls over the course of just a few months last year, created a breach with the country that has emerged as America's most active ally in dealing with the rise of extremism in Syria, Libya and Mali. Were the intelligence gains from monitoring French telephone data, and listening into some calls, worth the risk to that diplomatic partnership? Probably not, but it is not an issue that the NSA, or the US Administration, seemed to consider prior to the Snowden revelations.

The NSA will resist having its reach limited by diplomatic considerations; after all, its view is that the more information, the better the chance of picking up future terror or cyber attacks. "Terrorism and cyber are the two biggest threats we face," General Alexander said in October. But conducting surveillance programs are not cost-free, as President Obama learned when the president of Brazil cancelled her state visit to the US out of pique over the revelations of American interception of conversations conducted by Brazilian government officials and executives of state-run companies.

The effects go beyond diplomacy. Executives of Google, Microsoft, AT&T and Verizon, among others, all say that the disclosure of their cooperation with American intelligence agencies, even if that cooperation is forced by secret court orders, is undercutting their business around the world. It's easy for France, or China, or others to block business with any American firm suspected, rightly or not, of providing data or "back doors" to American intelligence agencies. "We have to think about how these programs hurt American competitiveness," one adviser to the administration said recently. "That's a question no one has seriously asked before."

- Many of the programs that the NSA has insisted on keeping secret might actually be accepted – and understood – if the instinct to keep secrets was tempered by a requirement to make far more public.

This thought is anathema to America's top intelligence officials, who say their success is closely linked to the secrecy of their operations. In some programs that is clearly the case: While it is no secret that the intelligence agencies work hard to listen into every critical conversation in Iran, Afghanistan, Pakistan and China, to name just a few targets, the revelation of how they do so only empower their adversaries to come up with new strategies to evade detection.

But there is a rising sense in Washington that the NSA took its instinct for secrecy to a harmful extreme. Suppose, for example, that the agency had publicly announced five years ago that it was beginning to collect a vast database of information about phone calls made in the US – the same information telephone companies hold for billing purposes – and would use it only to trace communications with terror suspects?

And supposing they had argued that such a database would have enabled them "to detect, and maybe stop, one of the 9/11 hijackers," as the former secretary of homeland security, Michael Chertoff, recently argued at a Harvard forum in Washington. If the oversight for the program seemed sufficient, it's likely most Americans would have accepted the government collection of that data as a necessary, if intrusive, defense against attacks.

Would disclosure have helped future terrorists? Probably not. It's hard to completely evade using phones, emails and Skype. And if they have been to the movies in recent years, they probably think the United States has far greater, speedier powers to listen into conversations or search emails than it really does.

Yet by keeping the programs secret, the NSA found itself on the defensive as soon as the Snowden revelations began. Its officials tried to justify surveillance programs that just months ago they denied existed. They had little credibility.

Some members of Congress attempted to force those revelations. Senators Mark Udall and Ron Wyden, both Democrats, sought permission to talk openly about NSA programs that they feared went beyond legal boundaries. Their request was denied – until the Snowden revelations forced the government to publish some previously-secret rulings of Foreign Intelligence Surveillance Court. Why couldn't they have published those rulings earlier? "We probably should have," one senior intelligence official said recently. "But it was never even discussed."

- The revelations about surveillance will make it harder to get international cooperation in stopping cyber attacks.

In their more candid moments, senior American intelligence officials concede they will soon have to make a choice: Is it more important to get a broad number of countries to join in monitoring global computer networks for cyber attacks than it is to collect information on phone calls, emails and web traffic in those same countries? That is the choice President Obama will have to make.

The simple fact is that the same technologies used to monitor the huge flow of data around the world – so that the US and its allies can protect against intellectual property theft or destructive, Stuxnet-like viruses – also enable the US to conduct extraordinary surveillance.

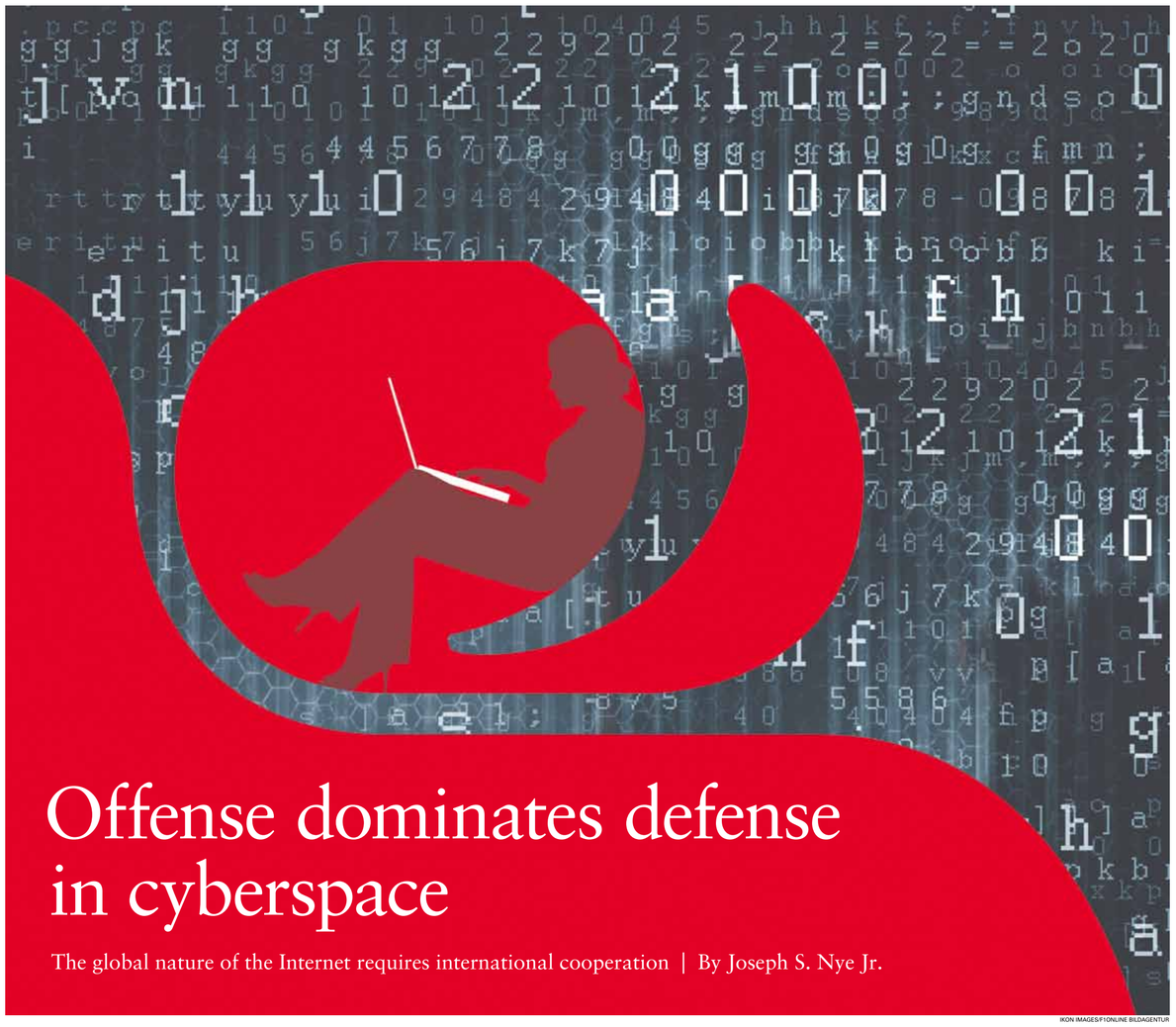
Look at one of the array of NSA programs to tap into the main cables that come into the United States, bearing much of the world's internet traffic. One of the best ways to stop Stuxnet-like viruses is to detect them flowing into one of those entry points in the United States. But that is also the best way to monitor email or phone call data.

If the US wants France or Israel or Turkey to join cyber-protection partnerships, it must assure them that the same technology will not be turned against them. Right now, the Snowden disclosures have sewn so much distrust that they threaten to undermine President Obama's cyber protection agenda.

All this suggests that the Snowden affair is hardly over. Its repercussions will be felt for years. But while General Alexander insists the problem is the disclosures themselves, his critics argue that the problem is the underlying programs. Over the past decade, America's sheer technological capacity to find needles in digital haystacks has improved exponentially. But the debate over how to use those powers is only beginning. And that debate is a global one; it can no longer be conducted among a small group of intelligence professionals and their lawyers. ■

David E. Sanger is the chief Washington correspondent of The New York Times and the author of "Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power."

PRIVATE



Offense dominates defense in cyberspace

The global nature of the Internet requires international cooperation | By Joseph S. Nye Jr.

IKON IMAGES/FOTOLINE BILDAGENTUR

General Martin E. Dempsey, chairman of the US Joint Chiefs of Staff, recently declared that cyber attacks had "escalated from an issue of moderate concern to one of the most serious threats to our national security. We now live in a world of weaponized bits and bytes, where an entire country can be disrupted by the click of a mouse." And while many nations now have military units dedicated to employing cyber in war, we may not be sure whether the hand on that mouse will be that of an official or a non-state actor.

The cyber domain includes not only the Internet of networked computers but also intranets, cellular technologies, fiber optic cables, and space-based communications. This domain is a complex man-made environment in which the barriers to entry are so low that non-state actors and small states can play significant roles.

The largest powers are unlikely to be able to dominate the cyber domain as they have others like sea, air, or space. Large countries may have greater cyber resources than non-state actors, but they also have greater vulnerabilities, and at this stage in the development of the technology, offense dominates defense in cyberspace.

Analysts of cyberspace are still not clear about the meaning of offense, defense, deterrence, escalation, norms, and arms control. At the same time, there is a danger of hyping the cyber threat.

The term "cyber attack" covers a wide variety of actions, ranging from simple probes, to defacing web sites, to denial of service, to espionage and destruction. Similarly, the term "cyber war" is used very loosely for a wide range of behaviors.

A more useful definition of cyber war equates it to hostile actions in cyberspace that have effects which amplify or are equivalent to major physical violence. If one treats hacktivism as mostly a disruptive nuisance at this stage, there are four major categories of cyber threats to national security.

Cyber war and economic espionage are largely associated with states: cyber crime and cyber terrorism are mostly associated with non-state actors. At present, the highest costs come from espionage and crime, but over the next decade or so, sabotage, war, and terrorism may become greater threats than they are today.

From what we can discern now, nuclear and cyber war would be enormously different experiences. Nuclear explosions are unambiguous and immediate; cyber intrusions can plant logic bombs in the infrastructure that may go unnoticed for long periods.

Moreover, cyber destruction can be disaggregated, and small doses of destruction can be administered over time. Even more dramatic is the difference in destructiveness. Unlike nuclear hostilities, cyber war does not pose an existential threat to humanity. As Martin Libicki of the RAND Corporation once commented, destruction of cyber systems could return us to the economy of the 1990s – a huge loss of GDP – but a major nuclear war could return us to the Stone Age. In that and other dimensions, cyber weaponry might be more appropriately compared with biological and chemical arms.

While there are many degrees of nuclear destruction, all are above a dramatic threshold or firebreak, and there has been a taboo against any nuclear weapons use for seven decades. In addition, although there is an overlap of civilian and military nuclear technology, nuclear technology originated in the war-fighting apparatus. In the cyber realm the web has burgeoned in the civilian sector.

> "The largest powers are unlikely to be able to dominate the cyber domain as they have others like sea, air, or space."

90 percent of military telephone and Internet communications travel over civilian networks. Finally, because of low costs and easy commercial access to the web, the barriers to entry to cyberspace are much lower for non-state actors than is the case in the nuclear realm.

Thus far, there have been no major crises in the cyber domain, though denial of service attacks in 2007 and 2008 on Estonia and Georgia and the Stuxnet malware attack on Iran give hints of what might come. In the area of industrial espionage, China has had a few incentives to restrict its behavior because the benefits far exceed the costs. Spying is as old as human history and does not violate any explicit provisions of international law.

While US-Soviet political and ideological competition limited the countries' cooperation in some areas, awareness of nuclear destructiveness led them to develop a crude code of conduct to guide the competition. Similarly, the two sides discovered a common interest in the issue of nonproliferation and began to cooperate in the mid-1960s.

Cooperation in the cyber domain is likely to follow an analogous course. There are already some institutions that relate to the basic functioning of the Internet, and a normative framework for cyber crime has already been started in the Budapest Convention. But it is likely to take longer before the major powers reach agreement on contentious issues such as cyber intrusions for espionage and for preparing the battlefield. Nevertheless, the inability to envisage an overall agreement need not prevent progress on sub-issues. For example, Russia and the United States agreed this year to establish various cyber security links "to reduce the mutual danger we face from cyber threats."

Many analysts argue that deterrence does not work in Cyberspace because of the problem of attributing attacks to specific actors, but that assertion is too simple. Interstate deterrence through entanglement and denial (i.e., defensive measures) still exists, even when there is inadequate attribution. Even when the source of an attack can be successfully disguised under a "false flag," governments may find themselves sufficiently entangled in symmetrically interdependent relationships that a major attack would be counterproductive. Unlike the single strand of military interdependence that linked the United States and the Soviet Union during the Cold War, the United States, China, and other countries are entangled in multiple networks. China, for example, would itself lose from a cyber attack that severely damaged the US economy, and vice versa.

In addition, an unknown attacker may be deterred by denial. If firewalls are strong, or the prospect of a self-enforcing response (an "electric fence") seems possible, attack becomes less attractive. Offensive capabilities for immediate response to a cyber attack can create an active defense that serves as a deterrent, even when the identity of the attacker is not fully known.

Futility can also help deter an unknown attacker if the target is well protected, or redundancy and resilience allow quick recovery. Moreover, attribution of the source of a cyber attack does not have to be perfect; to the extent that false flags are imperfect and rumors of the source of an attack are widely deemed credible (though not provable in a court of law), damage to an attacker's reputation may threaten its "soft power" and thereby contribute to deterrence.

Finally, a reputation for offensive capability and a declared policy that keeps open the potential means of retaliation can help to reinforce deterrence. Of course, non-state actors are harder to deter, and improved defenses such as preemption and human intelligence become important in such cases.

In the cyber domain, the global nature of the Internet requires international cooperation. Some people call for cyber arms control negotiations and formal treaties, but differences in cultural norms and the difficulty of verification make such treaties hard to negotiate or implement. At the same time, it is not too early to explore international talks and cooperation to try to develop rough rules of the road that can limit conflict. The most promising early areas for international cooperation are probably not bilateral conflicts but problems posed by third parties such as criminals and terrorists.

Cultural differences present a difficulty in reaching broad agreements on regulating content on the Internet. Russia and China have sought a treaty for broad international oversight of the Internet and "information security," banning deception or the embedding of malicious code or circuitry that could be activated in the event of war.

But the United States has argued that arms control measures banning offense can damage defense against attacks and would be impossible to verify or enforce. Moreover, the United States has resisted agreements that could legitimize authoritarian governments' censorship of the Internet.

Nonetheless, it may be possible to identify behaviors like cyber crime that are illegal across cultural and economic systems. Trying to limit all intrusions would be impossible, but one could conceivably start with cyber crime and cyber terrorism involving non-state third parties; there, major states would seem to have a joint interest in limiting damage by agreeing to cooperate on forensics and controls.

Historical analogies are always dangerous if taken too literally, and the differences between nuclear and cyber technologies are great. The cyber domain is new and dynamic, but so was nuclear technology at its inception. Nuclear learning was slow, halting, and incomplete. The intensity of the ideological and political competition in the US-Soviet relationship was much greater than that between the United States and Russia or the United States and China today. There were far fewer positive strands of interdependence in the relationship. Yet the intensity of the zero-sum game did not prevent the development of rules of the road and cooperative agreements that helped to preserve the concurrent positive-sum game.

Joseph S. Nye Jr. is University Distinguished Service Professor at Harvard's Kennedy School of Government.

TOM FITZSIMMONS

That is the good news. The bad news is that cyber technology gives much more power to non-state actors than does nuclear technology, and the threats such actors pose are likely to increase. The transnational, multi-actor games of the cyber domain pose a new set of questions about the meaning of national security. ■

A longer version of this article appeared in the September/October 2013 issue of the Bulletin of the Atomic Scientists under the title: "From bombs to bytes. Can our nuclear history inform our cyber future?"

It may be cyber but it's not war

Applying the military mindset to the fifth domain is counterproductive | By Thomas Rid

"Cyber war is coming!" proclaimed the RAND Corporation in an influential paper in 1993, exactly two decades ago. A dozen years later, by 2005, the US Air Force declared it would "fly, fight, and win" in cyberspace.

The future of war would surely play out in that "fifth domain," on top of land, sea, air, and space. Dark warnings of a "Cyber Pearl Harbor" soon became a staple of Washington discourse. Earlier this year, the Pentagon announced a five-fold staff increase at its Cyber Command, despite acute budget cuts. America, it seems, is gearing up for cyber combat.

But what would such an act of cyber war look like? History suggests three features: To count as an armed attack, a computer breach would need to be violent. If it can't hurt or kill, it's simply can't be war. An act of cyber war would need to be instrumental. In a military confrontation, one party generally uses force to compel the other party to do something they would otherwise not do. And an act of war would need to be political, in the sense that one opponent says: "Look, if you don't do X, we'll strike you; and if you don't comply, we'll strike again." That's the gist of two centuries of strategic thought.

No past cyber attack meets these criteria. Very few even meet a single one. Never has a human being been injured or hurt as an immediate consequence of a computer-attack. Never did a state coerce another state by cyberattack. Very rarely have state-sponsored offenders taken credit for an attack. So if we are talking about war – the real thing, not about a metaphor (as in the war on drugs) – then cyber war has never happened in the past, cyber war is not taking place at present, and all-out cyber war seems unlikely in the future.

Yet cyberattacks are already happening, both criminal and political ones. Indeed a computer breach could cause an electricity blackout or interrupt a city's water supply, although that also has never happened in the past. So if it's not war, what is it?

The politically most important attacks are either sabotage, espionage, or subversion.

Code-borne sabotage is a real risk. So-called Industrial Control Systems run all sorts of things that move fast and can burn: trains, gas pipelines, civilian aircraft, refineries, even elevators and medical devices. Many of these systems are highly vulnerable to breaches, and knowledge about some system vulnerabilities is easily available. Therefore the number of violent computer-sabotage attacks against Western targets may come as a surprise: Zero.

Why zero? Because causing havoc for a truly critical target through weaponzied code is harder than it looks. Target intelligence is needed. Control systems are often uniquely configured for highly specific tasks, and also incorporate plant-specific legacy components. This limits the possibility of generic attacks. That means potent attack software needs to be tailor-made. It also needs to be tested on real-life equipment. A case in point is Stuxnet, the famous attack against Iran's nuclear enrichment program.

The second threat is cyber-espionage. Data breaches are not just a risk, but a real bleeding wound for the United States, Europe, and other advanced economies. The bigger and more immediate problem is not the NSA violating the privacy of Americans and the country's allies. The bigger danger is that emerging markets in Asia are clandestinely sucking competitiveness and employment out of advanced economies via fiber-optic cable. How big these costs are is unclear; that they are big is certain. But espionage is not war, and cyber-espionage is not cyberwar.

GETTY IMAGES/ANTON MELLER/V

Finally there is subversion, using social media and other Internet services to undermine established authority. It does not come as a surprise anymore that subversives use new technologies, from Anonymous to Occupy Wall Street to Arab protesters all the way to militants and insurgents. Twitter and Facebook have made organizing non-violent protest easier than ever before, often in the service of liberty and freedom. It also should not come as a surprise that authoritarian regimes enhance their counter-subversion with new technologies and the Internet: spying on their citizens, arresting the troublemakers, both liberal and illiberal ones.

So what precisely is the problem with cyber war?

Talk of cyber war is misleading. On closer examination of the facts, the opposite of war is happening: computer breaches are less violent than old-style attacks, not more violent. Violent sabotage, Stuxnet-style, may have become harder if done through computer – but non-violent sabotage is now possible, easier, and it is happening more often: crashing websites, deleting files, and stealing negotiation strategies. The same goes for espionage: infiltrating software and opening remote backdoors is much less risky than infiltrating human agents and clandestinely bugging embassy walls.

Talk of cyber war is also disrespectful. Last year the US Department of Defense considered creating a new Distinguished Warfare Medal for drone operators and developers of computer attacks. Real combat veterans protested vehemently when they learned that the award would have ranked higher than the Purple Heart. Defense Secretary Chuck Hagel then scrapped the medal. Ending or saving the life of another human being is an existential experience; deleting or modifying data is not. Violence demands respect.

Talk of cyberwar kills nuance. Intelligence agencies have begun taking "cyber" seriously. By doing so, signals intelligence as well as human intelligence agencies are updating their tradecraft for the 21st century. The West is now beginning to have an overdue debate about what kind of intelligence activity is legitimate for a 21st century democracy, and where red lines should be drawn. Drawing these lines requires subtlety. It is therefore time for this debate to drop even the "cyber-" and call a spade a spade again: espionage, plain and simple.

Thomas Rid is a Reader in War Studies at King's College London. He is the author of Cyber War Will Not Take Place (Oxford University Press/Hurst).

PRIVATE

And finally talk of "cyberwar" is in the interest of those with a harsher vision of the web's future. Many countries are tempted to take control over their cyberspace, over their sovereign corner of the Internet. Especially authoritarian states like to tweak their technical infrastructure, their national laws, and their firewalls to "protect sovereignty in cyberspace," as they like to say – which in practice means protecting intellectual property thieves from foreign pressure and rounding up dissidents at home.

The armed forces need to stay focused on fighting and winning the real wars of the future. That's hard enough. Let us not militarize the struggle for the free and liberal Internet today. ■

We need norms

Cybersecurity is no longer a matter for individual states – it is an international issue | By Matt Thomlinson

Societies are increasingly dependent upon a global network of information and communications technology (ICT) to control the critical infrastructures and communications systems essential to modern life. ICT offers great benefits for states and their citizens alike – increased efficiency and transparency in government, improvements in civil society, and economic growth.

Yet along with these benefits have come new threats, including cybercrime such as identity theft and fraud, politically motivated attackers who threaten critical infrastructure, and sophisticated economic and military espionage.

ICT can also be exploited to cause significant harm. For example, a series of recent cyberattacks has disrupted the critical operations of major energy and financial companies. A 2012 attack against Aramco, a national oil and natural gas company, took

Matt Thomlinson is General Manager, Trustworthy Computing, Microsoft.

MICROSOFT

down 30,000 computers; and in 2013, an attack froze many of the computers of a major bank, affecting ATMs and mobile payments.

To respond, states are under significant pressure to develop and maintain capabilities for defending the nation in cyberspace; maintaining appropriate intelligence capabilities; enforcing criminal law; and reducing risk in its critical infrastructures and its broader economy.

Governments are acting to bolster the range of their national security capabilities in cyberspace. A study by the United Nations Institute for Disarmament Research (UNIDIR) in 2011 identified 33 nation states that address cyberwarfare in their military planning and organization, including "the use of cyber capabilities for reconnaissance, information operations, the disruption of critical networks and services, for cyberattacks, and as a complement to electronic warfare and information operations."

However, conflict in cyberspace, unlike physical warfare, does not have a widely agreed-upon set of conventions, or more significantly, norms, for regulating conflict. This potential for legal uncertainty, coupled with the technical difficulties of attributing cyberattacks to specific actors – whether state-sponsored or not – creates an opportunity for nation states to engage in a range of problematic behaviors, including espionage, surveillance, and attacks. State insecurity can also erode ICT innovation either by continued exploitation of ICT products in the name of national security, or through unnecessary regulation in an effort to reduce risk.

As a result, the need for diplomatic dialogue among nations has reached a critical juncture. Developing a global understanding of cybersecurity priorities is essential to the long-term stability and security of cyberspace, and requires collaboration among governments.

Unlike the historical evolution of international norms, the development of "cybersecurity norms" should also engage the private sector. While it is true that only nation states can create actual legal norms, a challenging aspect of the cybersecurity discussion is that a significant portion of the infrastructure of the Internet resides in the private sector. This affects cybersecurity discussions because some security actions are outside the control of national governments.

In many instances, previous efforts to build cybersecurity norms benefited from private sector technical assistance. The private sector influenced such agreements as the Missile Technology Control Regime, Financial Action Task Force on Money Laundering efforts, and the norms promoted by the International Civil Aviation Organization for civil air travel. The private sector was also vital in garnering critical congressional or parliamentary support for the ratification of these agreements.

Private sector experience and perspective would benefit international diplomatic discussions around cybersecurity norms, as it has been the private sector that has had to think through the technical challenges and priorities of securing billions of customers around the world.

The United Nations Office for Disarmaments Affairs (UNODA) recently released a report on Developments in the Field of Information and Telecommunications in the Context of International Security. It recommends: "While States must lead in addressing these challenges, effective cooperation would benefit from the appropriate participation of the private sector and civil society."

The discussion around cybersecurity norms currently centers on a wide range of themes. Some of these themes may not reach the status of international norms in traditional diplomatic terms, but they may well evolve into norms that benefit the development of positive behaviors among governments and ICT providers.

ICT companies around the world have a unique view of threats in cyberspace as they receive threat information from millions of computers, mobile devices and servers globally that have opted into anonymously sharing telemetry back to them. Many companies regularly publish their findings – Microsoft for example publishes its semi-annual Security Intelligence Report (SIR).

Based on this broad and long-standing cybersecurity experience, I have observed five important principles that should underlie international discussions of cybersecurity norms:

- Harmonization of Laws and Standards: Given the global and ubiquitous nature of the Internet, developing global cybersecurity laws and standards will promote understanding, predictability, and enable collaboration on problem solving among countries.
- Risk Reduction: Cybersecurity stakeholders should work to improve the security of the Internet through collective responses to threats by sharing information about threats and vulnerabilities, and by engaging in the active prevention of cybercrime.
- Transparency: Governments can help to build trust and increase predictability and stability in cyberspace by practicing greater transparency in their cybersecurity practices.
- Collaboration: As governments construct cybersecurity practices to address security concerns at the international level, they can seek input from a variety of stakeholders, including the private sector, civil society, and academia.
- Proportionality: The issue of proportionality is challenging, because it is not yet clear how proportionality in cyberspace will be interpreted. However, nations should begin to develop interpretations of proportionality in cyberspace under customary international law.

The international implications of cybersecurity are immense. How countries behave in cyberspace from a security perspective is no longer the private matter of an individual state; it is an international issue. Countries need to articulate a clear policy on how they approach security in cyberspace, and how they will organize to ensure their respective economic security, defense, and public safety as it relates to cybersecurity. To advance the international discussion, I am proposing a four-step process for driving the development and understanding of global cybersecurity norms and practices:

1. Prioritize issues in cybersecurity that require diplomatic engagement from an international legal perspective; identify ways to modify current international laws to incorporate changes caused by technology and innovation.
2. Analyze existing cybersecurity best practices and policies at the national, regional, and international level and determine where global principles or practices need to be developed. Key areas to explore should include confidence-building measures, responses to security incidents, assessment and mitigation of risk to critical ICT infrastructure, risk management, supply chain security, and protecting core encryption and trust mechanisms of the Internet.
3. Develop a set of cooperative measures for trust, stability, and reliability in cyberspace, with appropriate responsibilities for the public and private sectors, including at the international level.
4. Drive for consensus on the most important issues in cybersecurity, as legal processes take many years to develop and become established both domestically and internationally.

While development of some of these positions should be led by government, many policies and the confidence-building measures that can enable effective cybersecurity practices are highly dependent upon the cooperation of the private sector. We therefore need an inclusive global dialogue on the continued development of principles and norms that advance cybersecurity. ■

Surprise, surprise! Spies go cyberspace

If governments asked me, I'd tell them: Stop engaging in cyber-espionage | By Eugene Kaspersky

SERGEY NIVENS/FOTOLIA.COM

Hackers are stealing confidential information from computers all over the world right this minute. There's a chance it could be your computer they're targeting while you read this article. There probably hasn't been a time other than now when everyone had so many tangible reasons to be paranoid about their privacy and the protection of their communications.

The invention and development of the Internet and of mobile technologies have brought immense benefits to humanity, including effectively revolutionizing the way we communicate. But all this comes with a price tag. For centuries, if not millennia, governments all over the world have been investing heavily in armies of spies to steal secrets from other states; so it should come as no surprise that they are doing exactly the same thing today – in the relatively new cyberspace. As a result, in the last couple of decades this age-old trade has been becoming more and more digital – with more and more bespectacled geeks and fewer vodka martinis.

Last year Kaspersky Lab discovered the unprecedentedly sophisticated espionage malware dubbed Red October. It was a network that was stealing classified data from diplomatic, governmental and scientific-research organizations in dozens of countries. We believe that it would have taken a team of at least 20 highly skilled professionals to develop and run this system, which was operational since 2007. We still don't know who was behind it, and probably never will. What's most alarming is that there could be other similar systems fully operational right now.

The problem is at least as acute if not worse in the corporate sector. A survey conducted by B2B International in 2013 of almost 3000 IT professionals in 24 countries all over the world showed that an overwhelming 91 percent of companies experienced at least one external attack on their IT infrastructure in the last year, with 35 percent of companies experiencing data leaks as a result – a quarter of that being sensitive information.

Industrial and state cyber-espionage is a murky world, so it's hard to calculate just how much it costs the global economy. However, the damage can be estimated to run up to hundreds of billions of dollars. With regard to the US, Keith Alexander, the director of its National Security Agency (NSA), recently described the loss of intellectual property by US companies that is syphoned off by cyberspies as 'the greatest transfer of wealth in history.'

Identifying who is behind such attacks is practically impossible as attribution can only ever be guessed at. It could be units created by nation states (for example, we at Kaspersky Lab believe that North Korea was likely to have been behind the recent cyber-espionage campaign against South Korea called Kimsuky), or it may be groups of hackers selling their malware to governments and corporations or running it on their behalf. After the Red October network was exposed, the people behind it quietly shut it down. One can only wonder – and shudder at the thought of – what they decided to turn their attention to afterward.

Bulletproofing data is impossible; the aim should be to maximize data protection. But how?

First of all, networks that contain critically valuable documents ideally should not have a physical connection with the general corporate networks or with the Internet at all. A physical safety perimeter should be placed around them. However, I understand that in most cases such separation is hard to implement in practice, as for the smooth functioning of businesses and of government affairs sensitive information of course needs communicating – often and effectively. Thus, this approach is rarely used.

The most basic recommendations on how to secure oneself from cyber-espionage when one's networks are hooked up to the Internet are very straightforward. All software on all computers on the network should be kept up to date, anti-malware software should be installed (preferably capable of tackling zero-day software exploits), and no one should open attachments in e-mails from unknown sources. The latter rule is probably the hardest to enforce as cybercriminals are increasingly adept at disguising their malware-containing communications as perfectly legitimate ones.

I would like to be able to call on all governments of the world to stop engaging in cyber-espionage (just imagine – everyone living life in peace), but I don't, as none of them is going to take any notice. Cyber-espionage is after all just an extension of the eternal fight for limited resources and the "us vs. them" paradigm for maintaining standards of living.

Eugene Kaspersky is the founder und CEO of Kaspersky Lab, and a leading global expert in the field of information security.

PRIVATE

In the meantime, the bad news for companies and governments is that they can hardly feel that the 'confidential' data stored on their computers is safe at any time. The good news is that it's still relatively easy to protect oneself with basic security commonsense – making all but the most sophisticated of attacks prohibitively expensive to carry out. ■

IKON IMAGES/F1ONLINE BILDAGENTUR

Worldwide web divided

The Snowden affair spurs demand for an end to super power IT supremacy and for "technological sovereignty" | By Sandro Gaycken

News that Angela Merkel's mobile phone may have been wiretapped by the NSA propelled the Snowden affair unexpectedly back into the center of the German media and political debate. The US ambassador was summoned to the Foreign Ministry and German politicians of every hue voiced their concerns.

On this occasion, politicians and the media were in agreement. That contrasts with the cautious political reaction when the Snowden revelations first broke.

After the initial media furor, it seemed that nothing serious had really happened. A lot of hot air was generated in the first weeks, but for mundane reasons: The media was at a loss for stories. The German parliament was in summer recess and the affair fell right into the beginning of the German election campaign cycle. But despite the media interest, the average German on the street didn't seem to care much.

Even now, surveys exhibit only a very slight change of attitudes towards data protection. This lack of interest was something of a surprise. Many policy makers and activists expected outrage. But the public had apparently expected as much from the NSA. There seemed to be no sense of surprise, no emotional moment.

Germans only seem to be overly concerned about state surveillance if the state doing the snooping is their own. That sheds an interesting light on the country's usual preoccupation with data protection. At least a part of it seems to be more an attempt to cope with German history than a real concern about surveillance as such. So is it all over? No harm done? Far from it.

Underneath the visible layer of the loud yet finite media hurricane and the contrasting lack of public interest, anger has been simmering among many who are professionally involved with data protection or secrecy.

Data protection advocates finally had proof of something they had long feared. Officials immediately started to gather expert groups, and to lobby politicians to harden and to internationalize German and European data protection standards.

A first consequence of this effort has just surfaced. The Committee on Civil Liberties, Justice and Home Affairs (LIBE) has backed a reform of European data protection. The reform was due anyhow. But the NSA scandal made it a strong piece of legislation. Companies compromising customer data can be made liable for up to €100 million or 5 percent of their annual profits; law enforcement agencies are only allowed to gather data as long as basic human rights are respected; and European data can only be submitted to other nations if requests conform with European law.

But concern spread beyond circles where activists are concerned about the restriction of privacy; equally solid concern arose in authorities over the restauration of governmental communications; confidentiality. The NSA and other agencies party to the multilateral signals intelligence cooperation agreement called "Five Eyes" – signatories are the US, UK, Canada, Australia and New Zealand – seemed to be able and willing to get into anything. (Sweden, France and many others appear to take a similar approach.)

Parliamentarians and government officials suddenly felt intimidated, seeing their independence threatened. German companies immediately feared cooperation between the secret services and foreign companies on industrial espionage – and not without reason. The German Engineering Federation (VDMA) reported widespread concern among its members, who fear losses in the billions.

Sandro Gaycken is a Director in the NATO SPS Program on National Cyberstrategies and the former Cybersecurity Strategist for the German foreign ministry.

FU BERLIN

These concerns for secrecy triggered another debate over technological sovereignty. This has been on and off the political agenda without any resolution being achieved so far. Costs were too high, and there seemed to be too little demand. Now, however, there is strong demand coming from a wide range of stakeholders, including some in Germany.

Government institutions, politicians and companies are asking for sovereign clouds, sovereign data links, networking equipment and networks for computers and – as of late – for secure mobile phones. Some of the solutions on offer are made in Germany.

Many countries have announced an interest in German IT. A fair part of the world is fed up with its dependence upon superpower products from China and the US.

This layer of the problem generated a very interesting, yet barely visible impulse. Germany is carefully developing ambitions to become a new Silicon Valley. This is a common baseline in many current discussions. Government representatives stress the need for German solutions and the accompanying investments in research, education and development.

The Bavarian government will soon release one billion Euros for IT development, much of it on IT security. The German foreign ministry recently offered to help national IT-security companies to establish contacts in other countries.

Economic impulses are also stirring. Investors have started asking about opportunities in "German cyber." The telecom giant Deutsche Telekom has announced ideas like a national German Intranet for German-to-German e-mails. And – this is the real turnaround – no one is talking about costs anymore, only about opportunities.

The IT superpowers China and the US tend to smile benevolently when they hear stories like this. China considers itself too cheap to fail and the US considers itself too everywhere to fail. But new trends in IT might prove them wrong – especially the upcoming "embedded revolution" with computers to be placed in all kinds of machinery.

This new IT doesn't have to be highly sophisticated or extremely expensive; it can be cheap, yet still secure. It doesn't have to be highly performing or extremely cheap at the cost of safety and security. And experience with office IT and consumer electronics is not that important. All these traditional advantages of US and Chinese vendors are less relevant. In this field, the world could start from scratch.

Germany might be the country best positioned to embark on this mission. It has solid knowledge about technology and how to regulate it in general. It knows the machinery that will host embedded IT. It is modest in its intelligence activities, not active in industrial espionage and a trusted agent in many respects. And it has always been keen on proper engineering with lots of reliability, safety, security and durability built in.

This new theme is still far from reality. But it's in the heads of many German decision-makers and engineers. And this is the real, the more substantial and – for the US – probably the most devastating outcome of the Snowden affair: A market and many visions for an end to superpower supremacy in the field of IT. ■

Finding a middle way

The cyber debate in India | By Samir Saran & Abhijit Iyer-Mitra

India is uniquely dependent on the cybersphere – it is the chosen medium for the implementation of the country's socio-economic schemes. But this also exposes the country to a higher probability of cyber-attack, according to National Security Adviser Shivshankar Menon. "Commitments to plurality and democracy in the cybersphere have to be tempered by security considerations," Menon said. Discovering the golden mean is both an Indian and a global imperative. It was against this background that delegates met in New Delhi on Oct. 14 and 15 for CYFY 2013, the inaugural India Conference on Cyber Security and Cyber Governance.

Given the democratic nature of India and its sheer size, the solutions it chooses will have a seminal influence on the future of cyberspace. The underlying theme for most of the discussions was how to preserve the democratic nature of cyberspace while protecting it. An early consensus emerged that privacy and individual freedom would have to be balanced against the question of security of society as a whole. Thus, the state will have to be empowered, to some extent at least, to deal with the kind of social instabilities that can be generated in the real world through acts in the virtual domain.

The debate threw up some interesting nuances. One conference participant said surveillance was like salt – good in moderation, unpalatable in excess. But it is clear there are many unresolved issues, including the very definition of what privacy is and what it is that we are trying to protect.

The debate on the concept and limits of sovereignty in cyberspace was also combative. The central question was how to regulate a domain that is international in its operation through the exercise of national sovereignty. "Cyber governance is something of an oxymoron," said Kapil Sibal, Indian Minister for Communications and Information Technology, "and a re-imagined notion of sovereignty is essential to develop an effective cybersecurity paradigm." The dilemma here is the inherent conflict between national security and the necessity of international cooperation, which is to some extent based on countries ceding sovereignty and working with each other.

Another overarching theme, and one on which there was much less disagreement, was the role of the private sector. There seemed to be general consensus that the government's role was morphing from that of a regulator to a facilitator. Delegates emphasized the state's role in setting security standards to ensure the resilience of the net. Contrary to romantic notions of the Internet and social media destroying the existing state system, the reverse is true – the state is empowered more dramatically than ever before. However the question of providing or generating sufficient cooperation between the government, private sector and civil society proved especially thorny given the issue of trust and surveillance especially with regards to privacy.

Samir Saran is Vice-President at the Observer Research Foundation and the co-host of CyFy2013.

PRIVATE

Abhijit Iyer-Mitra is programme coordinator for the conference.

PRIVATE

Jaak Aaviksoo, the Estonian Minister of Education flagged the issue of the Internet "not being a virtual domain." There are physical aspects to it, he pointed out, and that means there are specific requirements in terms of how we build resilience into the system. He also raised the question of moral legitimacy, required to create a culture of trust building between the government and the people because the whole question of state versus citizen has been a central theme in the evolution of the debate on cyber governance.

India's own policy in terms of developing a layered approach was brought into focus – specifically the question of training large numbers of people to ensure that India's planned cybersecurity policy can be implemented. Deputy National Security Adviser Shri Nehchal Sandhu admitted that "while India has a national cybersecurity policy it is still to develop a national cyber-security strategy."

The sheer size of India's cyber-population makes its national deliberations critical to the global dialogue. The key discussions here revolved around whether to promote sovereignty on the net or even to seek a wholly sovereign Internet. Are we going to side with those who say information security is absolute, or those who say each government has the absolute freedom to do what it wants in its own territory.

That India is finding its own middle way was best reflected by the fact that, despite furious debate, there was little to no mention of PRISM or Snowden. Being pragmatic it would seem India and Indians, unlike the EU or Brazil, have chosen to forgo rhetoric and instead debate the core issues around privacy, anonymity, intellectual property and national territoriality.

One final question that came up was whether technological developments would allow states to dominate. This is a debate that has played out historically in every new medium that has emerged. As the international negotiations proceed in the coming years, the whole question of whether we are going to have an internet that is transcendental and collectively used across the world or is it going to be dominated by each country in its own little domain of influence.

The India conference was the start of a process – one that raised many questions and found some interesting and out-of-the-box answers. The complexity of the debate dictates that this will not be an easy path to navigate. The India Conference on Cyber Governance and Cyber Security will not and cannot be a one-off interaction among multi-stakeholders. It is the beginning of a strong forum that can debate India's policies, help mould its strategy and simultaneously address global challenges. ■

Cyber security
A continuous challenge

By John Suffolk and Ulf Feger

PICTURE-ALLIANCE/DPA/DAVID EBENER/PETER MASTIC

Cyber security is an issue of intense interest to our customers, governments, and vendors alike with the topic frequently being in the headlines. Indeed it is probably accurate to say cyber security has never been higher up on the global news agenda.

The high interest reflected in the intense coverage and attention could lead to the misleading thought that we are facing something fundamentally different than before. However, the issues that need to be solved with the global information, communications and technology (ICT) infrastructure have not changed much in recent years. In fact, the challenges are rather structural and deep-rooted.

The question that we need to find a common answer to remains the same: How can we reduce the risks to people, companies and governments in our ICT system when it is, by its nature, global, interconnected and therefore fiendishly complex to untangle and safeguard?

Just to give you a hint on how global technology is: Up to 70 percent of the components of the technology portfolio of Huawei are not from Huawei itself, but from a global supply chain, with US companies being the biggest provider of components at 32 percent. Most other companies have similarly complex supply chains. That means we will all need to consider the challenges beyond the confines of our own company if we are to strengthen the security of our networks and products.

It is a widely shared view that global questions can be answered only on a global level. Yet for decades well-intentioned words from technology companies have led to little progress. We believe it is only by working together internationally, as vendors, customers, policy and law makers will we make a substantial difference in addressing the global cyber security challenges. We also believe that we must share knowledge and understanding of what works and what does not work to reduce the risk of people using technology for purposes never intended.

If there was a simple answer or a solution to the cyber security challenge it would have been found by now, and it would have been adopted. However, the sheer fact that the world continues to debate standards, laws, codes and norms tells you we are all at the early stage – we must share what works, so others can adapt and improve.

The time has come to elevate this beyond the level of companies and make cyber security a priority for international, inter-governmental institutions. In the 21st century cyber security is vital for all the aspects of life that in previous centuries would have forced governments to come together to thrash out a resolution. From economic well-being to national security, cyber security impinges on areas that are the proper domain of diplomats, not just company CEOs, however powerful.

It might seem a little excessive to compare cyber security and the threat we faced by nuclear weapons over many decades. But the issues are not radically different and the approach to tackling them remains a sound one. Collaboration at the highest levels of diplomacy is the best way to make significant progress on complex problems.

Attempts to create true uniformity at international standardization have failed up till now. In the last 20 years the global ICT industry has exploded around agreed global technical standards and disciplines – everything from hypertext to WiFi – but when it comes to cyber security many standards are just not standard or even exist.

It is time to press the reset button on the security challenge and ask ourselves if we wish the future to be different from the past, and indeed today, in what way will we work together to define and agree new norms of behaviour, new standards, new laws and create a new realism in the balance between privacy and security.

The more governments, enterprises and technology vendors can detail common standards, understand their purpose and the positive difference they make and commit to their effective adoption through buyers using their buying power, the more the world will begin to see a difference. This is not about solving every problem, but it is about having a common agreement about what problems we are trying to solve and how they should be solved.

While we urge governments to work together to make more progress on advancing cyber security, it also remains absolutely incumbent upon ICT firms to show progress themselves.

In this regard Huawei's white paper on cyber security, which was released on October, 18 provides detailed information about its end-to-end cyber security approach, including a practical overview of the approach Huawei takes to the design, build and deployment of technology that involves cyber security considerations, including overarching strategy and governance structure, its day-to-day processes and standards, staff management, R&D, security verification, third-party supplier management, manufacturing, delivery and traceability.

The white paper is a small contribution to our collective knowledge and we have written it to help people understand some of the policies, procedures and transformations that vendors such as Huawei are considering in relation to cyber security. We recognize we still have much to do to continuously improve our approach. However, our commitment to openness and transparency drives everything we do and we believe the more people who review, consider, assess and question our policies and procedures, the greater the promotion and impact on our ability to deliver better quality products and services.

At Huawei we are willing to work with all governments, customers and partners to jointly cope with cyber security threats and challenges in order to enhance our capability and effectiveness in designing, developing and deploying secure technology.

Huawei continues to believe that the world is a better place when the innovations brought about by the use of technology are maximized, they improve people's lives, and they improve economies. Huawei will continue its open and transparent approach and responsible position to its operations and everything it does. ■

John Suffolk
Senior Vice President and Global Cyber Security Officer of Huawei Technologies

Ulf Feger
Cyber Security Officer of Huawei Technologies Deutschland GmbH

About Huawei

Huawei is a leading global information and communications technology (ICT) solutions provider. Through our dedication to customer-centric innovation and strong partnerships, we have established end-to-end advantages in telecom networks, devices and cloud computing. We are committed to creating maximum value for telecom operators, enterprises and consumers by providing competitive solutions and services. Our products and solutions have been deployed in over 140 countries, serving more than one third of the world's population.