The Security Times

SPECIAL EDITION OF THE ATLANTIC TIMES FOR THE FIRST GERMAN CYBER SECURITY SUMMIT

September 2012 Berlin, Germany

New Uncertainties

By Theo Sommer

FOTOLIA/URMOMENTS

These days we no longer have enemies on our borders. Moreover, there are currently no armed conflicts between states. Nonetheless the present era is characterized by uncertainty and instability. "There are fewer military threats to our territory, but more challenges to our security, from every direction," says NATO's Secretary General Anders Fogh Rasmussen. But what, concretely, are those threats and challenges?

NATO sums it up thus: proliferation of weapons of mass destruction, cross-border terrorism and organized crime; regional crises, genocide and climate change; danger to vital trade routes, especially maritime routes; cyber-attacks on our data centers and deep sea data cables; attacks on pipelines, nuclear power stations, stock exchanges or transport systems; conflicts about water, natural resources and energy supplies. Epidemics and pandemics are often included in the list, as well as growing migration flows.

NATO would be the defense tool of choice for only a few of those risks and threats. Most cannot be dealt with by deploying armed forces. This is certainly true for pandemics. The same goes for organized crime: in the final analysis it is a policing problem.

Terrorism continues to be a challenge to be taken seriously, but its nature has changed. Religious radicalism is still virulent, but after the loss of its Afghan base and the liquidation of bin Laden, al-Qaeda has lost its significance as the operational hub of global terrorism. It is geographically fragmented into independent sub-units primarily interested in local issues. In the future, surgical use of force to combat terrorism can supersede military interventions leading to protracted ground wars.

Anyway, the Arab Spring has taken quite a lot of wind out of the jihadists' sails. Nowadays the biggest threat emanates from home grown terrorists – young people radicalized in their native countries in the West. Again, they are more a matter for the police and the domestic intelligence services than for the armed forces.

What about the proliferation of nuclear weapons? A look at the past decades tells us three things.

First, proliferation is happening more slowly than experts assumed 30 or 40 years ago. Apart from the five UN veto powers (the US, Russia, Britain, France and China), only four states have so far made it into the nuclear league: Israel, India, Pakistan and North Korea.

Second, countries that feel threatened, or rogue states continually under the menace of regime change, can hardly be stopped even by the most draconian sanctions from setting up an arsenal of nuclear weapons – witness North Korea, and perhaps Iran.

Third, if proliferation cannot be prevented through sanctions, a lethal military strike is hardly the right answer. An Israeli attack on Iran would cause havoc in an already highly unstable region. And the Iranians, should they really go nuclear, surely know that their own destruction would be the price of any attack, either on Israel or on Western Europe. Even ayatollahs will defer to the logic of the balance of terror: he who shoots first will inescapably be the second to die.

Climate change is another story. The consequences of global warming are droughts, famines, rising sea levels, the disappearance of island nations and the acidification of the oceans. Climate change might trigger climate wars, especially over water. Civil war could become the norm in many areas, and violence can be expected to spill over borders into other countries and continents. In 2010 the National Security Strategy of the Pentagon underlined this analysis: "The danger from climate change is real, urgent, and severe. The change wrought by a warming planet will lead to new conflicts over refugees and resources."

The armed forces come into their own whenever climate change leads to new cockpits of confrontation. This could be the case in the Arctic where the ice is melting at a breath-taking speed. If the Northwest Passage and the Northeast Passage from the Atlantic to the Pacific were to become permanently navigable, it would considerably shorten the sea routes to Asia. This in itself might incite a maritime arms race.

Matters are complicated even further by the fact that under the Arctic Sea there seems to be a rich treasure of oil, gas and other natural resources. Since the territorial claims of the five littoral states overlap, controversies are unavoidable. So far the Arctic countries have been in a cooperative mood. But it is already becoming apparent that they will be backing up their claims with military hardware.

Elsewhere, too, the quest for natural resources may culminate in conflict. The insatiable appetite of sovereign states for the supplies they need is bound to acquire ever greater significance. But business competition could easily turn into political rivalry, even strategic confrontation. It should be the task of diplomacy to prevent this.

When it comes to what is probably the biggest new threat, cybersecurity, the problem is rather different. This is an area in which the armed forces have an important role to play. After all, the Internet was a product of US defense research. And as in every war, soldiers will play a crucial role in any cyberwar.

Yet not everything that tends to be called cyberwar is really war. It is important to draw some distinctions. Stopping the Internet "hacktivists" is a non-military issue. Likewise, cybercrime – stealing credit cards, siphoning money out of bank accounts, data theft on the Web – is a matter for the police.

Cyber-espionage is a much more serious affair. Here it is important to draw a distinction between spying on the business secrets of private companies and the classic kind of spying that involves the official secrets of government authorities and the military.

In the recent past, institutions ranging from the office of the German chancellor to the Vatican, the White House and the Church of Scientology have been the targets of cyber-attacks. Companies in the private sector (which own and operate between 85 and 95 percent of the critical information infrastructure) have repeatedly been the victims of cyber attacks, among them Sony, Google, Morgan Stanley, CitiBank, Lockheed Martin and Boeing.

Continued on page 2

Science fiction becomes reality

By René Obermann, CEO Deutsche Telekom

René Obermann is Chief Executive Officer of Deutsche Telekom.

DEUTSCHE TELEKOM

The first Cyber Security Summit aims to set the course for Germany as a safe place to do business. These days, no country on earth can remain competitive without highly developed information and communications technology. Connecting all areas of the economy and society must and will gain ever more speed. As a consequence, the networks become a critical infrastructure – and the target of attacks. Therefore, providing the best possible protection has to be the common goal of the business sector and the state.

Cyber-attacks taking down power grids or financial markets, or rerouting airplanes, are no longer merely the stuff of science fiction. They are a real threat. Crime is increasingly moving online in the 21st century. Cybercrime has become an industry in its own right. We're not "just" talking about the theft of personal data; we're talking about organized crime and industrial espionage at a professional level.

The constantly growing threats to our connected world call for a whole new dimension in networked defense. Everyone involved knows there can never be 100 percent security on the Internet. But together we can do a lot more to substantially increase the level of security.

The Cyber Security Summit is addressing this objective to the decision-makers in business and politics for the first time, to establish a dialogue on the current dangers and on the structures for closer cooperation. ■

Cyberspace and security

By Wolfgang Ischinger, Chairman Munich Security Conference

Ambassador Wolfgang Ischinger is Chairman of the Munich Security Conference.

PRIVATE

Last year, writing about the intersection of cyberspace and security, the former NSA and CIA director Michael Hayden remarked, "Rarely has something been so important and so talked about with less clarity and less apparent understanding."

Recent developments and revelations have only made this statement more pertinent, both when it comes to attacks against states and against private-sector entities. The so-called "Olympic Games" program aimed at Iran and its nuclear program, which included the Stuxnet virus, was the first destructive cyber-campaign of this kind in history. And the number and severity of cyber-attacks on states and companies is increasing by the day.

Yet, it is still difficult to grasp some of the most fundamental issues: What does cyber mean for international security? How can we best protect our critical infrastructures and our businesses? What legal frameworks, what partnerships between private sector and government make sense? We are only just beginning the conversation.

On cyber-security, much work remains to be done on the level of experts. However, since we first placed the issue on the agenda of the Munich Security Conference (MSC) in 2011, we have also realized that we need more high-level exchanges. For this reason, we have decided to expand and deepen the debate, bringing German stakeholders together, in cooperation with Deutsche Telekom, for the Cyber Security Summit. I anticipate very productive discussions in Bonn. ■

BILDAGENTUR HUBER/IMAGETEK

– quo vadis?

By Klaus Wittmann

There are those who believe that NATO has served its purpose. This is true in so far as the Alliance successfully achieved the task of maintaining security during the Cold War. But it does not mean it no longer has a role to play. Since the fall of the Berlin Wall, NATO has embarked on cooperative, as opposed to confrontational, security policy, adopting in November 1991 the strategic concept of a "strategy without an adversary."

As someone who has been involved in NATO's continued transformation since 1990, this author has often expressed concerns about NATO: sclerotic bureaucracy; lack of frank debate and fresh ideas; glossing over of divergent views; predominance of military thinking; difficulty in finding agreement about the nature of "new" security challenges; overextension, weakness of the European members.

Yet, it is going too far to question the very existence of NATO. After its first alleged "identity crisis" in the early nineties, the Alliance has changed in ways unimaginable at the time of the one-dimensional threat from the Soviet-led Warsaw Pact. And in several regards it has demonstrated enduring relevance.

In the three phases of its history, the Alliance safeguarded Europe's security during the East-West conflict, helped consolidate and stabilize Central, Eastern and Southeastern Europe after the end of the Cold War, and took on peace missions beyond its area of mutual assistance after the terrorist attacks of September 11, 2001.

However, this common chronological division should not be misinterpreted. The tasks of each new phase have not simply replaced the old ones - they have complemented them. Ensuring the protection of member states' territory, populations and forces continues as a permanent mission even without any concrete adversary. Much remains to be done to achieve a Europe "whole and free." And out-of-area missions will again be asked of NATO, even if there is currently a degree of intervention-weariness after the extraordinary Afghanistan effort. These enduring tasks are reflected in the three "core missions" laid out in the (third) Strategic Concept of November 2010: defense, cooperation and crisis management.

PRIVATE

Brigadier General (ret.) Klaus Wittmann is a Senior Fellow with the Aspen Institute Germany.

Transatlantic defense

True, in the new world disorder many security challenges are not of a mainly military nature. Cyber threats, endangered energy security, terrorism and organized crime, failed states, the effects of climate change, resource competition and the like cannot be countered by predominantly military means.

But they all have security implications and are worth discussing in a political and military security organization – and one which, to date, is the only such body with teeth. In these areas, it would be important for NATO to work out precisely where it can add value to the efforts of the international community.

In addition, given the emergence of new actors and the existence of various smoldering conflicts and other threats to the global commons, it is not possible to predict when or where NATO members' security and interests may be challenged in the future. Seen in this light, the Alliance is an insurance policy – and one whose sheer existence may even prevent the materialization of direct threats.

NATO is not a solo player on the international scene, but part of the concert of security-relevant organizations, the so-called "interlocking institutions." However, the old insider joke about "interblocking institutions" aptly illustrates the over-ambitiousness, competition and jealousy that frequently seem to prevail over the drive to achieve complementarity, cooperation and synergy.

What NATO has to offer specifically is its integrated military and command structure, decades-long experience in military cooperation and interoperability with partners, as well as joint force and operational planning. It should not seek to do things that the European Union, for instance, can do better – and vice versa. But it should be a part of a comprehensive approach tying together civilian and military efforts, without aiming to dominate other organizations.

Among the factors required to convincingly establish NATO's continued relevance is an open and ongoing debate about the raison d'être, the role and functions of the Alliance, and also a greater consensus about the assessment of threats. The new Strategic Concept with its elegant consensual formulations is not the final word.

Consensus should continue to govern NATO decision-making, but the principle of "coalitions of the willing" could be institutionalized so that these do not appear as a stopgap solution for lack of a common course.

Stronger political will is needed for the achievement of ambitious goals, particularly in Germany, which must not (as in the case of Libya) allow pacifist sentiment and fear of public opinion to cause a turning away from Alliance solidarity.

Lessons must be drawn from recent foreign missions particularly in Afghanistan, where NATO was left with a task assumed in theory by the wider international community. Important initial mistakes were made: a regional concept and early reconciliation efforts were lacking; goals were over-ambitious; improvement in Afghan living standards too slow. Thus the legitimacy of "nation building" by external forces has increasingly become questionable.

The transatlantic link must be kept strong. But with Washington's more pronounced Pacific orientation it is clear that Europeans (in NATO and in the EU) need to take more responsibility for the security of the European continent and its periphery. The consequences for defense budgets as well as for "smart defense" (including Pooling and Sharing of capabilities) must be faced and explained to the public. Greater European influence depends on adequate contributions.

The new balance established in the Lisbon Strategic Concept between collective defense and out-of-area missions still lacks concrete definition and implementation – NATO must concentrate on its core tasks and follow a sharply focused defense and security agenda. Global partnerships are useful, but they must be developed with utmost transparency and should not imply that NATO is "going global".

The Alliance should also play an active part in the development of a meaningful future arms control and confidence-building agenda.

The NATO-Russia relationship demands greater efforts. In a common search for Russia's place in the European security order, NATO should vigorously demand from Moscow new, cooperative thinking in its security policy (as part of the much-evoked "modernization"), while self-critically acknowledging its own share of responsibility for the worsening of the relationship over the last 15 years.

One aspect appears key: In the globalized and diffuse security environment, "broadened and intensified" consultation among Allies as pledged by the Strategic Concept is of the essence. This means rigorous application and a wider interpretation of Article 4 of the Washington Treaty, which obliges the signatories to "consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened." Therefore it would have been logical to add "Consultation" as a fourth "essential core task" to the triad proclaimed in the new Strategic Concept.

Expanding this concept will mean a genuine cultural shift in NATO. Until now, many obvious security issues have never reached the Council table, not least for fear that disagreements would be interpreted as an internal crisis, or that consultation about a given subject would be read as an implicit tendency towards military intervention.

Finally, NATO urgently needs to better communicate its purpose and explain its continued relevance in an era so different from its founding epoch – not only after summit meetings and not in bureaucratic 65-paragaph declarations. ■

continued from page 1

These kinds of attacks may be irritating and troublesome, but they do not constitute aggression in the sense of a full-scale cyberwar. However, such wars have already occurred, and NATO is rightly concerned that in future they will increase in number and effectiveness.

The first Internet attack in history occurred in the Baltic republic of Estonia early in 2007. In a three-week cyber-blitzkrieg the country's computers were overwhelmed by a data tsunami that brought the financial industry to the verge of collapse. It is suspected that the Russians were behind it.

A year later it was Georgia's turn, and it was probably not an accident that it occurred at the precise moment that the Russian army was moving toward Tbilisi. The government's computers and those of the media crashed, and President Mikheil Saakashvili had to switch his website to an American server.

The cyberwar that has raged for some time between Israel and Iran is on a different scale. In the first battle in this conflict, which it is generally believed Israel and the United States prepared for in painstaking detail for years, a sophisticated computer worm by the name of Stuxnet put the centrifuges in Natanz, the Iranian nuclear enrichment facility, out of action, led to a series of technical mishaps in the nuclear power station Bushehr, and brought the uranium conversion facility in Isfahan to a standstill.

Our vital infrastructure has become more and more dependent on online networks. If they are shut down by cyber-attacks, it could lead to a complete breakdown of public life.

The areas affected would be the transport sector, the electricity, water and gas supplies, the civil and military communications system, and the railways and airlines. Chemical factories could explode, satellites would gyrate out of their orbits, and stock exchanges and banks would have to close. GPS would no longer be available, so our navigation devices would suddenly cease to function. In one fell swoop, online warfare thousands of miles away would become impossible. US Secretary of Defense Leon Panetta has called this kind of devastating attack a "digital Pearl Harbor." Other people have called it an "electronic apocalypse."

For this reason it does not come as a surprise that by now almost 150 states have embarked on cyber-programs, and that the armed forces in particular are gearing up to fight a computer war. In this area the Pentagon spends half a billion dollars annually, and the new Cyber Command has a staff of 10,000. (Germany has had its own cyber-defense center since 2011. But it's miniscule staff of 70 cannot be expected to do more than superficially coordinate the work of various government departments.) NATO has recently begun to address the issue. A Computer Incident Response Center, the Cyber Defense Center of Excellence, which is located in a former Red Army barracks in Tallinn in Estonia, and a number of other NATO institutions are training people for cyber-warfare and attempting to heighten cyber-awareness within the Alliance.

What is the proper response to a cyber-attack? Should it be construed as an act of war from the outset? In the new US defense doctrine, cyberspace is listed as the fifth potential theater of war after land, sea, air and outer space. President Obama has declared America's digital infrastructure to be a strategic national asset, and Pentagon spokesmen have hinted that the response to a cyber attack may well be a classic military retaliatory strike.

Yet how does one retaliate if it is impossible to ascertain the address of the aggressor? Where attribution is impossible, a doctrine of retaliation is of little use. And deterrence will not work. NATO is still trying to come to grips with this question.

The Alliance should not succumb to cyber-war hysteria. Nor should it exaggerate the danger of cyber-terrorism out of all proportion. Hitherto there has not been a single case of a terrorist web attack, and as yet no car bomb and no explosive belt has been detonated via the Internet.

Moreover, we should resist the comprehensive militarization of cyberspace. The armed forces have to ensure the security of their own online systems, but they should not be granted a monopoly over the entire area of cyber defense. Here the state, the business community and the armed forces must act together closely, with policymakers taking the lead.

NATO will not be able to renounce cyber weapons altogether. However, there is a need for arms control even in the IT world. If cyber-diplomacy wishes to make its mark, it should try to achieve an international consensus concerning the behavior of states in virtual space and at the same time to establish guidelines and regulations on how to deal with non-state actors, dangerous hackers and digital terrorists.

Almost until the end of the 20th century, security meant primarily one thing: safeguarding one's own territory against external military aggression. This territorial notion is largely out of date. Today what tends to be at stake is human security, unobstructed supplies of energy, natural resources and foodstuffs via open trade routes, the protection of the environment and the preservation of the climate. These are all survival issues, which can be dealt with only through very close cooperation between policymakers, business, civil society, national authorities and international institutions.

No longer are our armed forces in a position to deal with the entire spectrum of risks, dangers and threats. They still have a vital role to play. But as new actors and diverging ideologies challenge the Western order, the primacy of statecraft is becoming ever more imperative. ■

ARCHIVE

Theo Sommer is executive editor of "The Security Times" and "The Atlantic Times" and Editor-at-Large of the German weekly DIE ZEIT.

Future challenges

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: September 7, 2012

PICTURE ALLIANCE/SUEDDEUTSCHE ZEITUNG PHOTO/ALESSANDRA SCHELLNEGGER

'A year of continued crises and stagnation'

Wolfgang Ischinger, Chairman of the Munich Security Conference, sees considerable risk of escalation in Iran, Pakistan and Afghanistan. He regrets the international community's failure to deal with the Syrian crisis.

THE SECURITY TIMES: Earlier this year you said that 2012 promised to become an exciting year in terms of foreign and security policy. Have your expectations been met?

WOLFGANG ISCHINGER: From a European and a global point of view, 2012 threatens to go down in history as a year of continued crises and stagnation. For different reasons, including the US elections, this year is not likely to see any progress on critical foreign and security policy issues.

Can you name three urgent security issues that are currently on your mind?

We have to differentiate between European and global issues. The future of the European Union and its ability to act on foreign affairs and security matters, including the future of the Eurozone as a model for a forward-looking policy of integration, is in the process of being sorely tested.

Thinking globally, I consider the developments in the Near and Middle East – from Syria to Iran to Pakistan – to be the most pressing security challenge right now. Moreover, I very much regret that the US-Russian "reset" of 2009 has come to an unfortunate standstill. I hope that in the aftermath of the US elections, the relationship between Washington and Moscow can be revitalized and with that also the relationship between NATO and Russia.

The reset has not really failed yet?

To a certain degree, the reset has been successful. Just think, for example, of the new START agreement on disarmament. On decisive questions of cooperation between East and West, however, we have not made any progress, especially with regard to Syria and joint missile defense. All we can do is wait and see until after the elections in the United States.

You consider the Near and Middle East one of the greatest security challenges. Are we facing a security meltdown in this region?

I do not see a meltdown. But what I do see is a continued crisis involving a considerable risk of escalation, not only in the case of Iran, but also in the completely unsettled crisis situation in Pakistan and Afghanistan. In Afghanistan, I am not really expecting the situation to develop positively after the withdrawal of Western armed forces. In the case of Syria, it is a shame to see the international community proving itself completely incapable of taking any action. This is a poor outcome so far both for the UN Security Council and for global governance as a whole.

How do you see the further evolution of the Arab Spring?

The developments in the Arab world must still be seen as a step forward and not as a step backward. Their path will lead from the old authoritarian regimes and dictatorships to other forms of government. It is, however, an illusion to believe that these other forms will automatically be those of liberal constitutional democracies as in the West. We must always remember that in many Western states democracy took decades, sometimes even centuries to develop. We need to show strategic tolerance here.

Germany's abstention in the Security Council vote on Libya raised great doubts about Berlin's reliability as a partner, in particular in the Anglo-Saxon countries.

Unfortunately, the collateral damage caused by this process was considerable in the initial phase. But I do not think that our reputation has suffered permanently. However, I do not think it is helpful to dwell on the difficulties of the Libyan situation. Instead, we should take as active a part as possible in stabilizing the situation in Libya and the surrounding area, especially in Mali.

The European Union is currently going through its worst crisis ever. Mountains of debt and a trend toward national retrenchment are threatening the process of continued European integration. Will we find the strength to make a fresh start and take the next step toward a political union?

I very much hope that we still find the strength. EU citizens must be told what the ultimate destination of their Union is going to be. In the years of crisis, we have discussed too many short-termist individual steps and have not focused enough on the long-term goal.

How can the younger generation be convinced that further steps toward European integration are needed?

The problem is not that our young people are turning away from Europe. They feel European and take Europe for granted – as though it had always been this way. We must remind them that present-day Europe is the outcome of six decades of stupendous effort. Without the European Union and its painstaking toil toward more and more integration, we would still be immersed in ancient enmities and be surrounded by barriers.

> "In the case of Syria, it is a shame to see the international community proving itself incapable of taking action."

Shaping the future of transatlantic relations is another topical issue. As a "Pacific President" Barack Obama belongs to a new generation of American leaders – one that is increasingly turning its attention from Europe to other world regions. How can we Europeans make ourselves heard in Washington again?

This is the million-dollar question, although not an entirely new one. When a new president is elected, we regularly wonder what we can do to make sure that our interests are taken into consideration in Washington. This has always been extremely difficult and will not become any easier in view of the new US "pivot" to the Asia-Pacific. We must realize that the United States takes Europe for granted as a partner, just as young Europeans take for granted a Europe without borders. But we should be glad that we in Germany need not feel threatened any longer and that the US president no longer needs to worry about Germany.

So how should the transatlantic partnership of the 21st century be defined from a European point of view?

The transatlantic partnership is like a plant: it does not thrive and prosper if it is not watered and tended regularly. It is in need of attention. We should, therefore, take care of this relationship not only in specialized circles of transatlantic diplomacy and defense cooperation. Moving forward, we should consider the market and our business enterprises as the actual backbone of the transatlantic partnership. If there are discussions in East Asia about establishing free trade areas, it is high time for us to finally tackle the idea of a transatlantic free trade area, a concept that has been bandied about for quite some time already. This would be the inspiring new element that could give our relationship new energy, new momentum and new power.

Are our traditional institutions and decision-making processes in foreign policy matters still adequate to meet the complex challenges of today?

It is about time to raise the question whether the classic division into foreign ministry, ministry of defense and various other ministries still makes sense. The lines between external and internal security, for example in the field of cyber security, are becoming more and more blurred. We should think about more adequate new forms and structures. In addition, the Germans have a very specific problem: our decision-making process in foreign and security crises is still improvable.

How would you reform the German decision-making process?

We need a National Security Council to process relevant decisions more systematically. In a time when Germany is expected to provide contributions even in situations where the lives of military personnel are at stake, preparing for such decisions requires a procedure of maximum precision and accuracy. Like our partners, we need a more systematic organization to achieve this. However, establishing a National Security Council should not have the effect of transferring all power to the Federal Chancellery. In accordance with the German constitution, important ministerial responsibilities should be preserved and even strengthened.

What does that mean for the much-touted "Parlamentsvorbehalt" – the legal requirement for the Bundestag to mandate and approve every military action?

As confirmed and specified by the Federal Constitutional Court, this requirement must be respected. However, it should be interpreted and applied in a way that does not restrict the ability to meet Alliance commitments and take action. The German government must be able to take executive action. Why not think about a parliamentary right of "co-determination" similar to the one granted to the legislature within the scope of euro crisis management?

The outcome of current deliberations about the "Parlamentsvorbehalt" should be an optimum ability to take action and not a maximum potential to delay action. This will require a fundamental consensus in society. And derived from that, the question will be whether we in Germany will ultimately be able to even conduct such strategic debates on foreign and security policy issues.

In September the Munich Security Conference hosts a "Cyber Security Summit" in Bonn in cooperation with Deutsche Telekom AG. What do you expect from this summit?

Two years ago, the Munich Security Conference began dealing with cyber-security and the risks stemming from cyber-threats for state, economy and society. I am glad that Deutsche Telekom has requested the Munich Security Conference to be a partner in tackling this novel spectrum of threats.

What precisely can foreign and security policy do to enhance cyber-security?

We all know that this is not only about defense mechanisms. In many places people are already working on the offensive use of cyber-technologies. Isn't it time to put a stop to the "digital Wild West"? I don't think it is too far-fetched to compare this problem with the problems that emerged in the 1950s and 1960s in connection with a possible deployment of nuclear weapons in space.

So you are pleading for an arms control approach?

At the time, it was possible to make all parties involved realize that it was in the best interest of all states to refrain from militarizing space. Irrespective of such obvious difficulties in the cyber field as attribution and verification, it is important to think about technical, political and legal options, the development of international conventions or the establishment of supervisory organizations.

Today we have a global suborganization of the United Nations for environmental issues. We must ask ourselves whether the ITU, the International Telecommunication Union, could tackle these new issues, or whether a new organization might be needed to seek adequate solutions. ■

The interview was conducted by Oliver Rolofs.

The pooling-and-sharing myth

So far, it's been mostly talk and no action. The European Union's 27 "Pentagons" need to get serious

By Hilmar Linnenkamp

CREATIV STUDIO HEINEMANN/IMAGEBROKER/OKAPIA

Does every defense minister need an air force? In times of budget austerity task-sharing is the logical solution.

The military instruments of the much-heralded Common Security and Defense Policy (CSDP) are expensive. The annual bill amounts to roughly €190 billion in defense budgets for 2012. This treasure is shared by 27 ministries of defense, 20 separate air forces with combat aircraft, numerous headquarters, gigantic logistical machineries, more than 20 defense colleges – and so on and on.

The European taxpayer has been too patient with governments and parliaments wasting resources on duplication and non-coordination. The 27 defense establishments own and operate 35,000 armored vehicles, no less than 2,300 fighter aircraft, more than 2,500 helicopters, and around 130 large combat ships – carriers, destroyers and frigates.

From these numbers alone, and from the fact that the equipment is unevenly distributed across Europe, it should be fairly obvious that there are typical strengths and weaknesses, overcapacities or capability gaps – a situation, in which more cooperation, more specialization and task-sharing is the logical solution in times of budget austerity.

Yet, the reality is still disappointing. Much has been said, researched, written and solemnly declared about Pooling and Sharing – little has been done, so far.

Over the last two years several NATO Council decisions seemed to promote the principle. But no sooner had the EU, in particular through the European Defense Agency, generated a stream of ideas and projects for more cooperation through P&S than NATO came along and hijacked the concept, selling it at the Chicago summit in May 2012 under the banner of the "Smart Defense Initiative," channeling it into its bureaucracy – and soon after almost forgetting it. The concept is too technical, has not achieved political visibility or momentum, and the wider public doesn't care.

There is another gap between reality and concept: Whilst P&S as a capability development tool is underestimated it does in fact work in the reality of coalition operations. In Afghanistan, for example, US helicopters fly injured soldiers of many nationalities out of harm's way; allied nations benefit from reconnaissance gathered by many other contributors; proven procedures allow commanders to ask for air support.

Actual combat is indeed a common effort, and resources are shared. But preparing for it – through focused development and procurement of equipment, through common training or shared logistical capabilities to be employed together – remains a national prerogative. National plans for Satcom services, ships, aircraft and ammunition are largely untouched by the obvious challenge of fighting together.

It's not all gloom, though. There has at least been some progress lately with regard to standardization and commonality of major equipment The Leopard II tank, the A400M transport plane, Eurofighter (a four-nation endeavor after the three-nation Tornado combat plane), the NH 90 helicopter entering service in 14 countries – all these projects look like progress of cooperation with all kinds of logistical and operational advantages.

At first glance it seems as if the much-needed "harmonization of military requirements" is being successfully implemented. A closer look, however, reveals that there is no joint maintenance program for the A400M nor do its crews train together – the only exception being the conclusion of a few bilateral arrangements.

The planned production of around 600 Eurofighters stresses the finances of the procuring partners, but no concept has been developed of cascading some of them down to allied air forces eyeing seductive offers from the United States to join the F-16 club of European member states.

Similarly the NH90 is supposed to be a joint helicopter project, yet it turns out that, 15 years after its maiden flight, there are more than

Hilmar Linnenkamp advises the research division International Security at the Berlin Institute for International and Security Affairs. From 2004 to 2007 he was Deputy Chief Executive, European Defense Agency.

SWP

Burden sharing

20 versions, making common servicing or crew training extremely difficult.

Breaking the stalemate of far-reaching declarations on P&S on the one hand and their irrelevance for the practical development of common and shared capabilities on the other requires a bold change in attitude among conservative and risk-averse military bureaucracies. Three options appear promising and realistic:

First, creating the conditions for shared support, training and economies of scale in the procurement process by a serious effort to reduce the diversity of weapon and support systems: cross-border acquisition, based on international competition, promotes commonality. After all, the US Navy buys German anti-mine drones. European armies may well coordinate their purchases of armored vehicles from a competitive selection of Finnish, Swiss, French or German design. And why not decide on a single model of the future military radio system?

Second, testing the benefits of common equipment with the well-established EU Battle Groups. If a core group of member states were to provide a permanent stock of equipment – from armored vehicles, helicopters, radios all the way to a field hospital – rotating personnel from all contributing countries would train and exercise this Battle Group. Such a system would represent an innovative version of „multinational" troops – no longer based upon an ad-hoc patchwork of national contingents with their own fighting materiel, but benefitting from shared standard equipment and services.

Finally, real progress on P&S needs political and public visibility beyond the military-technical details of its engineering. Hence, a limited number of identifiable lighthouse projects should be considered. Two obvious candidates would have to be brought to the attention of the long-suffering European taxpayer: All crisis management operations (not only military!) under CSDP need reliable and affordable communications systems. Why, therefore, not establish a shared EURO-Satcom system that, in ten years from now, can replace the individual military satellite communications capacities operated nationally today?

Furthermore, air policing – already a small island of cooperation under NATO with regard to the Baltic airspace – could be organized collectively on the basis of a Euro-Air Defense Force. Thus, a core group of Member States would provide a standing multinational force of fighters to protect regional airspaces in peacetime and develop, in this way, cooperative experience and effective procedures for common operations?

There is a way forward on Pooling and Sharing. But it needs the attention and engagement of finance ministers and, of course, the heads of government to persuade the 27 European pentagons to get serious. ■

Spreading the risk, sharing the costs

How to make the German military part of an integrated security structure without bypassing parliament

By Andreas Schockenhoff and Roderich Kiesewetter

The Eurozone debt crisis is stealing Europe's voice. The debate over how to save the common currency is smothering discussion of other, urgently needed reforms. These include changes in EU foreign and security policy, precisely because funds are in short supply. In the future, no EU member state will be able to finance the entire spectrum of military and civilian capabilities alone.

Yet a coherent, independently robust and credible Common Security and Defense Policy (CSDP) is attainable only if policymakers dare to implement more European integration. Three premises provide the foundation for our remarks:

In the future as now, Europe will not be able to safeguard its own security. It will still need American support, despite the recent US turn toward Asia.

Europe must enhance its own effectiveness while ensuring that it again becomes a relevant partner for the US. That includes anchoring NATO as a foundation of transatlantic relations.

States prepared to strengthen Europe must be ready to share the risks and to share the obligations as their capabilities allow. Those not prepared to do so must accept less influence.

An effective CSDP can succeed only if EU member states relinquish part of their national sovereignty, just as sovereignty is currently being ceded in financial and economic policy. That is the extent to which the military capabilities of individual states must be integrated and placed under shared leadership. The concerns of individual nations will no longer carry as much weight.

Also, we must launch a substantial debate over what the EU's civilian and military missions can achieve. As a point of reference within Europe, Germany can act as a mediator here. Berlin should conclude pooling and sharing agreements with willing partners, especially in mutual air defense, common coastal defense, joint training facilities, command structures (such as the EU and NATO Headquarters in Ulm) and a unified command and information system. All this could be prepared by a joint EU/NATO working group at the political director level, whose jobs should include determining concrete working fields for joint agreement and necessary relinquishments of sovereignty.

The question of further ceding national rights will also continue to occupy the Bundestag, which has relatively strong rights in regard to military matters compared to other European national parliaments. The Bundestag should agree to changes to the requirement for parliamentary approval of foreign military deployments. Parliament must retain the last word as a right of recall. But making Germany's decision-making process more flexible would do much to build confidence among our partners.

Andreas Schockenhoff is deputy chair of the CDU/CSU parliamentary party responsible for foreign, defense and European policy.

DEUTSCHER BUNDESTAG

Roderich Kiesewetter is CDU/CSU parliamentary spokesman for disarmament, arms control and non-proliferation.

DEUTSCHER BUNDESTAG/ H.J. MÜLLER

Foreign deployment

What's important is that both we and our allies should have reliable access to "shared" command, logistical, intelligence and training units. The example of AWACS flights makes clear how vital the reliable provision of Bundeswehr troops and military capabilities are for a credible and sustained operation, especially as Germany supplies 40 percent of the leadership and specialist personnel.

The President of the German Bundestag and leaders of the parliamentary party groups must begin to discuss the possibility of a more flexible approach. One option might be an annual debate of security policy guidelines in the Bundestag. It should end with a plenary debate and a vote on a parliamentary resolution providing German soldiers and capabilities for integrated armed forces.

Deployments would be subject to a unanimous resolution of the European Council (or the NATO Council). That would give the executive the "right of deployment." The Bundestag – the legislative – would hold the "right of recall."

This suggestion for changing German deployment law should be promptly reviewed for its conformity with the constitution. Possibly, parliament would have to pass additional legislation.

Pooling and Sharing agreements should become enshrined in security policy guidelines. After parliamentary approval, the German government would have a mandate to deploy the earmarked forces and means within the framework of the agreements without having to seek the Bundestag's approval. Here, too, parliament would hold a right of recall. ■

This article is an excerpt from a longer paper that appeared in the September/ October 2012 issue of Internationale Politik.

Iranian President Mahmoud Ahmadinejad inspecting the Natanz nuclear plant.

PICTURE ALLIANCE/DPA/EPA/IRAN'S PRESIDENCY OFFICE

Tehran's nuclear balancing act

Iranian leaders must realize that failing to limit the enrichment program will eventually trigger war | By Mark Fitzpatrick

As summer draws to an end, a diplomatic solution to the Iranian nuclear crisis remains nowhere in sight. Despite cyber-attacks, sabotage, other forms of clandestine warfare, and, most importantly, sanctions that have halved oil sales, Iran continues to enrich uranium at an ever faster pace.

The new quarterly report by the International Atomic Energy Agency (IAEA) records further alarming figures: Iran's enriched uranium stockpile will grow to nearly 7,000 kg, enough for over four bombs if further enriched, and more of it will be at the 20 percent enrichment level that is a short step away from weapons grade. More centrifuges will be in place and more enrichment work will be taking place at the deeply buried facility at Fordow, out of reach of Israeli bombing.

Israeli officials made exaggerated claims in early August about a new US intelligence estimate assessing greater Iranian progress toward weaponisation than earlier thought. The US still concludes that Iran has not resumed the weapons work it suspended in late 2003. Yet work on the other two elements necessary for a bomb continues apace: stockpiling fissile material and perfecting a missile delivery system. Sanctions have impeded progress in the solid-fueled missile program and prevented Iran from enriching uranium even faster with advanced centrifuge models, but neither program has been halted.

Meanwhile, the optimism that greeted the initiation of talks in April between Iran and the six powers (France, Germany and Great Britain plus China, Russia and the US, dubbed the E3+3 in Europe but the P5+1 in the US) led by EU foreign policy chief Catherine Ashton quickly dissipated. Although crippling EU and US sanctions brought Iran to the negotiating table, they were not enough to persuade Tehran to offer more than a halt to 20 percent enrichment, for which it asked an exorbitant price: the lifting of sanctions and an acknowledgement of Iran's right to enrichment.

In addition to a halt to 20 percent enrichment, the six powers have demanded two other initial steps by Iran: exporting the accumulated stockpile of 20 percent enriched product and shutting down Fordow. In exchange, the Six offered to supply 20 percent enriched uranium fuel for the Tehran Research Reactor, assistance with reactor safety and aircraft spare parts. Unsurprisingly, Iran judged this opening negotiating position to be unacceptable. Although President Mahmoud Ahmadinejad said last autumn that Iran could halt 20 percent enrichment as a quid pro quo for reactor fuel, Iran since then has produced fuel on its own (whether it is safe to use is another matter), and now seeks a higher price.

If Iran were to indicate it could go along with 'stop, ship and shut,' then the E3+3 would have to consider whether to respond with some sanctions relief. But so far, Iran has not tested the unity of its negotiating partners by giving any reason for them to consider compromise. Iran is only willing to consider stopping the 20 percent enrichment; no ship and no shut. The artful characterization by some Iranians, such as former Iranian negotiator Hossein Mousavian, that the E3+3 offer amounts to seeking to trade 'peanuts for diamonds' greatly distorts the respective negotiating positions.

If Iran were willing to consider a complete suspension of uranium enrichment – as demanded by six Security Council resolutions – and exporting the stockpile of not just 20 percent enriched uranium but also the 3.5 percent enriched product, this would indeed be equivalent to diamonds. For such a compromise, the US and allies should certainly offer equivalent concessions in return. But the 20 percent product is only a small part of the problem. It is the most urgent aspect of Iran's enrichment program, because continued production at Fordow could spark the premature Israeli attack that the US desperately seeks to forestall. Yet some perspective is needed about the 20 percent issue. The 20 percent stockpile is currently not close to being enough for one weapon, and a third of the stockpile has already been converted into a fuel-precursor form that makes it harder to use for weapons purposes. The crux of the matter is not the relatively small amount of 20 percent enriched product, but the larger stockpile of 3.5 percent enriched uranium and the ever increasing production rates. This is why Israel has not been happy with the E3+3 focus on 20 percent enrichment, fearing that this position can become an implicit acceptance of enrichment at the lower level. Quick to label the summer talks a failure, Israeli policymakers seemed almost pleased that Iran rejected the E3+3 gambit.

Mark Fitzpatrick is Director of the Non-Proliferation and Disarmament Program at the International Institute for Strategic Studies in London.

INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES

Flashpoint IRAN

As perceptions harden that diplomacy has failed, apprehensions heighten over the possibility of an Israeli air strike this autumn. Judging from their words, Prime Minister Benjamin Netanyahu and Defence Minister Ehud Barak want to give the strike order in the next two months. Yet there is intense push-back in Israeli security circles over the inadvisability of unilateral action. And it is impossible to determine how much of the Netanyahu/Barak rhetoric about military options is a bluff to persuade Iran to step back.

Iranian officials project nonchalance about the possibility of air strikes, judging that Israel could not do much damage on its own and that the US would not be willing to join. The former may underestimate Israeli capabilities and the latter is only true for the moment. President Barack Obama drew a clear red line this spring when he said a nuclear-armed Iran is unacceptable and that he was not bluffing about using a military option to prevent it. The unstated corollary to this position is that he would accept an Iranian nuclear capability as long as Iran does not cross the line to production. Obama cannot say so explicitly for fear of being labeled an appeaser, but such a position is merely a statement of fact. By most definitions, Iran already is nuclear capable – now possessing all the materials and technology, requiring only a political decision – and, while unpalatable, this status has not triggered military action.

The problem is that the red line separating nuclear-capable from nuclear-armed will become less clear as Iran's enrichment program makes further advances. At present, Iran is still months away from being able to make a successful dash to produce weapons-grade highly enriched uranium (HEU). Because IAEA inspections take place on average twice a month, any such 'breakout' at declared facilities would be detected in time.

If, however, the Iranians sought to produce HEU at clandestine plants, they could not be confident the work would remain hidden. Twice already, secret enrichment plants have been exposed. Iran might judge that it could get away with such exposure, claiming, as it does today, that it does not need to follow IAEA rules about early notification of new nuclear facilities.

If this is Iran's calculation, it could well backfire. Iran does not know how close it could come to crossing the line to weapons production before its adversaries determined it was too close. If Iran's enrichment program continues unabated, at some point Western intelligence agencies will judge that because the uranium stockpile is too large, the technology too advanced and the hiding places too many, a dash for the bomb cannot be detected in time. The red line of weapons production will have become too blurred to serve as an effective tripwire.

There are many reasons to oppose military action against Iran, not least of which is that air strikes probably will not set back Iran's program for more than two to three years. They may even spur Iran to produce nuclear weapons faster than would otherwise be the case, and then also without IAEA inspectors on the ground to gauge progress.

If Iran is already judged to be crossing the line to weapons production, however, the argument of counterproductivity fades away. Iranian policymakers should understand that failing to limit the enrichment program will eventually trigger war. ■

Months? More like decades

An attack on Iran would be illegal and impossible to contain | By Michael Lüders

In the armed conflict with Iran that by now seems nearly inevitable, two scenarios are emerging. The Israeli leadership could opt to attack Iran before the US presidential elections on November 6, thereby forcing the Obama administration, in the midst of the election campaign, to reluctantly stand by its Israeli ally militarily. Refusing to do so would substantially hurt Barack Obama's prospects for a second term. The Republicans, closely aligned with the Israel lobby through their largely fundamentalist Christian voters, would delight in painting Obama as a weakling.

Alternatively, the Netanyahu government could receive a firm commitment from Obama for a US-led attack next year. That would be the Israeli side's final offer. In both cases, the Iran conflict would remain on the agenda. Most Western analysts believe that the Israeli saber-rattling of the last few weeks has been designed solely to ratchet up the pressure on Tehran via Washington. This view comes up short, however.

Michael Lüders is a political scientist and Islamic studies scholar and a former Middle East correspondent for the German weekly Die Zeit. He is the author of "Iran: Der falsche Krieg" (Iran: The Wrong War).

PRIVATE

Flashpoint IRAN

Why would Israel raise the pressure? The latest round of negotiations on the Iranian nuclear program, begun in Istanbul in April between the 5+1 states (the permanent members of the Security Council plus Germany) on the one side and Iran on the other, have been failing to make progress chiefly because Israel, acting through the Americans, has been blocking every negotiated solution. The Iranian side has offered to stop enrichment beyond five percent – to date it has enriched up to 20 percent. Five-percent enrichment is not enough to build a nuclear weapon. In return Tehran wants Washington to ease the sanctions imposed on the Iranians.

Only at first glance is this conflict about Iran's nuclear program. Israeli Defense Minister Ehud Barak has admitted in several interviews that an Israeli attack would set back Iran's nuclear program by only a few years, and certainly not destroy it completely. But that was an acceptable outcome, he added, because additional time would be gained to topple the Iranian regime.

Although neither US nor Israeli intelligence can deliver proof that Iran is working on a nuclear weapon, Netanyahu's rhetoric of a looming second Holocaust has created a kind of virtual reality in which facts hardly play a role anymore. Gideon Levy, an op-ed writer for the newspaper *Ha'aretz*, the last journalistic bastion in Israel to categorically oppose attacking Iran, has called Netanyahu a "messianic, megalomaniacal warmonger" who has lost all grip on reality when it comes to Iran. Seen in this light, an illegal war of aggression against Iran could well begin before the US elections. There is almost no public debate in the West about the possible consequences. That could prove a grave omission because such a conflict would last not weeks, as the hawks maintain, but years or maybe even decades. ■

Israel's war of nerves

Attacking the Islamic Republic's nuclear facilities would be folly – yet Israel may have no other choice | By Josef Joffe

This MOP isn't for cleaning floors. It stands for Massive Ordnance Penetrator, the most powerful explosive device in the American arsenal – six meters long and weighing 14 tons. The monster bomb is built to bore through concrete 60 meters thick before its 2.5-ton explosive charge detonates. It would be the weapon of choice to wipe out the deeply bunkered Iranian enrichment facility at Fordow, near Qom.

Why Fordow? It is a military restricted zone, fenced by anti-aircraft guns and rockets. The International Atomic Energy Agency (IAEA), the UN's nuclear watchdog, had no idea this underground project existed. It was discovered three years ago by Western intelligence services. Ever since, the fear has been that the Iranians are working in two-track mode: Over here, you see the inspected installations; over there, we have their clandestine counterparts.

When Fordow was uncovered, the US Air Force ordered MOPs. The first were delivered last fall. Yet Defense Secretary Leon Panetta is not certain that the thing actually works the way it's supposed to. "We're still in development," he said earlier this year. The mountain rock above the centrifuge rooms is at least 60 meters thick. Maybe the MOP will chew its way through, maybe it won't. Would a second device manage the final meters? The planners remain optimistic: Either way, they say, the highly fragile centrifuges wouldn't survive the shock.

One thing's for sure: the three-year-old war of nerves keeps escalating. An attack wasn't a question of days or weeks, but not of years either, said Israeli Prime Minister Benjamin Netanyahu last March. Amos Yadlin, the former chief of AMAN, Israel's military intelligence, claims to know the date. In the *New York Times* he oracled that Israel would unleash its forces on the day "when Iran is on the verge of shielding its facilities from a successful attack."

Is "when" really the only question that matters now? As Israeli diplomats and intelligence officials tell anyone who'll listen, the time for diplomacy is running out. Then the weapons will do the talking. Of course, sanctions and the on-again-off-again negotiations with Iran might yet breach the wall of refusal. What if they don't? The sources shake their heads ruefully: for an attack, the weather is still fair.

Israel is waging psychological warfare. Political pressure is preferable to blast waves that could engulf the entire Middle East. All the more reason to examine the cold facts. Israel's problem is the hardware. The Americans have it, starting with the MOP and the long-range B-2 bomber to deliver it. They have the air bases encircling Iran and the aircraft carriers cruising the Persian Gulf. Their hundreds of jets could decimate the Iranian air defenses, destroy the command bunkers, wipe out the coastal batteries and rockets that could deliver retaliation against the world's oil artery. Above all, they could keep what strategic analysis jargon calls "escalation dominance" – if Iran doubles the stakes, the US can quadruple them. The hotheads in Tehran know that.

If they act along even remotely rational lines, they will not go to war against the US, for instance by responding to an Israeli preventive strike by attacking Saudi Arabia or tankers in the Gulf. Iran could loose its proxies – Hezbollah and Hamas – against Israel, but they, too, would have to closely calculate, given that Israel holds escalation dominance in the region. Would they really want to die for the mullahs in Tehran?

In the wider arena, however, Israel does not hold this dominance. This is the weak point of all attack scenarios discussed in the media. The Israelis have one of the world's biggest air forces, even bigger than France's or Germany's. But it's built for the shorter distances of the Middle East neighborhood. Necessarily bearing the brunt of the operation would be two airplane types originally intended for air-to-air combat: versions of the US-built F-16 and F-15, with an "I" for "Israel" as an appendage. These are capable of longer-range operations.

Yet even this extended arm is too short. Just how long it is remains the secret of the Israeli Air Force (IAF). Combat radius also depends on the flight profile, payload and time spent over the target. For example, if an F-16I "Storm" flies very high in very thin air, with extra fuel tanks it can cover 1500 km. Yet if it flies low to evade radar in Jordan, Iraq and Iran, its combat radius shrinks by half.

A target for Israeli or American missiles? The deeply bunkered Iranian enrichment facility at Fordow, near Qom.

PICTURE ALLIANCE/DPA/DIGITALGLOBE/HANDOUT

The F-15I "Thunder", the IAF's mightiest jet, probably has similar specs: 1000 to 1500 kilometers. And yet, no matter how you twist it, it's not enough. The pilots would have to turn back about a hundred kilometers short of the enrichment sites at Fordow and Natanz. If they were to fly on anyway, they would have to refill their tanks over territory that's not exactly friendly: Jordan and Iraq using the direct route; or, on the northern variant, along the Syrian-Turkish border. They could fly undetected only over the sea, around the Arabian Peninsula. That would mean 5000 kilometers: an absurd venture.

A perfect alternative, however, would be a fourth attack corridor from Azerbaijan. This northern neighbor of Iran is Israel's new friend in the Islamic world. Iran was lost in 1979; Turkey in the last few years. Rumors have been circulating since March that Baku is considering handing four old Soviet-era air bases near the Iranian border over to the Israelis. From there, the route to Isfahan would be only half as far as from the Mediterranean. Still, this option, too, must be filed under "war of nerves." If Azerbaijan becomes Israel's staging ground, it can expect fearful retaliation from Iran. The categorical denials from Baku are hardly surprising: "There will be no operations against Iran from our territory."

Geography, then, remains Israel's foremost enemy, one that can be overcome only by mid-air refueling. Yet Israel has only five tanker jets, modified Boeing 707s. Time for some mental math: The IAF has 100 Storms and 25 Thunders. If they're all deployed at once, they would have to be refueled twice, on each leg of the mission. 125 times two equals 250 – with a handful of tankers?

Then with half the fleet, perhaps? That wouldn't change much either, because bombers have to arm themselves against fighters and ground-to-air missiles. The Iranians' 50-odd fighters (F-14s, Mirages and MiG-29s) may be old to obsolete, but still have to be reckoned with. Escorts need to come along. Iran's anti-aircraft defenses also aren't up to date, because the Russians flatly refuse to deliver the latest version of their S-300 system. Yet the danger remains acute in the immediate vicinity of the target sites, where anti-aircraft installations are especially dense. The Israeli bombers would require an advance guard to shoot open the last few miles. It follows that about a hundred jets would be required; a figure in utter disproportion to a few tanker jets.

Yet a strike force that size would not be too big, given the list of targets. Here are the top eight:

Ardekan – a uranium factory under development in Parchin) carrying it can fly.

Fordow – a highly fortified enrichment facility, covert until 2009, that enriches uranium to 20 percent, almost seven times more than that required for civilian nuclear reactor fuel.

Arak – a heavy water reactor due for completion in 2014. A "primary target" because it uses natural uranium, which breeds highly fissile plutonium.

Natanz – a 100,000-square-meter enrichment site, eight meters underground and shielded by massive concrete walls.

Bushehr – originally a German reactor begun by Shah Reza Pahlevi, now completed by the Russians, which likewise produces plutonium. However, because of unpredictable fallout, Israel will not risk bombing a "hot" reactor.

Darkhovin – an Iranian reactor project due to go online in 2016, but currently still "cold."

This short list omits dozens of laboratories and research sites that are paving the long road to the bomb, whether through basic physics research or breeder-reactor chemistry.

As simple as the targets are to identify, they are vexingly hard to hit. Firstly, without refueling the Israelis could reach only Arak. Secondly, unlike the Americans, they could not conduct a bombing campaign lasting weeks that would steamroll through all resistance – anti-aircraft defenses, air strips, command centers – before the actual targets were attacked.

Would that suffice to rule out unilateral Israeli action? Not necessarily, because the Israelis don't fight American-style, relying on overwhelming force, firepower and duration. Instead, they might disable some links in the bomb-making chain, by singling out Isfahan, for example: no uranium gas, no enrichment; no metallic uranium, no bomb. For good measure they might take on Natanz, where they could bust the bunkers without needing MOPs.

And then?

In March the Pentagon leaked the outcome of a wargaming simulation to the media, in which a unilateral Israeli attack delayed the nuclear program by only one year while unleashing war throughout the region. The scenario included an Iranian counterstrike with rockets that hit a US Navy vessel in the Gulf, killing 200. That would be the point at which the Americans would launch their own war against the Islamic Republic. And still, the time gained amounts to only two more years. It's no use.

Whether the Iranian program is set back three or ten years depends, of course, on the extent of the destruction ordered by the US president. The Pentagon's indiscretion carries a political subtext. The military does not want a war against Iran, which is why the generals passed the unsatisfactory results to reporters. President Obama doesn't want war either. That was why he gave the Turkish premier a message to pass on to Iran's supreme leader Sayyed Ali Hosseini Khamenei. It said that a "civilian nuclear program" would be acceptable if Khamenei could demonstrate convincingly that Iran would "never seek nuclear weapons," as he himself claimed in a televised speech in February.

If all negotiations fail, would Storm and Thunder take over? Not even the Israelis really want to take it that far, opinion polls suggest. Only 19 percent support a unilateral strike without the US. Two thirds are against. One third even opposes any kind of attack. These are not figures reflecting enthusiasm for war. The government's own thinking moved on years ago, which is why it has opted for German Dolphin submarines. They are deterrents, not first-strike weapons. And, unlike land-based jets and Jericho missiles, they are practically invulnerable. That is exactly why the Schröder and Merkel governments have delivered them: Better to have an Israel that can mount a credible strategic deterrent than one that, in the moment of existential crisis – kill or be killed – is the first to push the button.

And what about the Iranians? Make no mistake: they have been working resolutely toward a nuclear option since the 1990s. With their nuclear sites, they can acquire all the necessary components for their own nuclear device. Analysts call that a "bomb on the shelf." Anything kept there could be quickly assembled and placed into an available delivery system.

The time remaining has become a popular guessing game – one year, two, three? If the regime hasn't secretly smuggled eight kilos of plutonium or 20 kilos of uranium into the country, the bomb is still a while in the future. Israel and the West actually started waging war long ago – diplomatically and in the dark. The weapons are sanctions, sabotage and bomb attacks on Iranian scientists – an Israeli specialty used to good effect against Nasser's Egypt and Saddam's Iraq. Since 2010, three big explosions have been recorded in Iran: two in missile storage sites, one at the Isfahan uranium conversion site. The sanctions' bite is causing pain. In July the US tightened them further.

Josef Joffe is co-publisher of the Hamburg weekly Die Zeit and teaches International Relations at Stanford University.

VERA TAMMEN

Flashpoint IRAN

It's a war of nerves, because the instruments used ahead of wars have not been exhausted. For Iran, the option of not just being able to build a bomb, but actually going ahead with it, remains only one scenario. And if it's chosen? "Even in the very worst case," meaning only a few months left before an Iranian bomb, "the president still has time to react," the *Washington Post* quoted a senior official as saying. By now the US is surely working on a MOP-2 capable of busting even the bunkers in Fordow. And by threatening attacks, the Israelis will keep applying the pressure that saves them from actually going to war. That guarantee expires as soon as Khamenei actually commissions a bomb. ■

This article originally appeared in the weekly Die Zeit.

Turkey, a role model

Islamist parties from Tunisia to Morocco aspire to be like the AKP. Turkey's governing party is also a close US ally

By Michael Thumann

PLANPICTURE/KAREL MESS

If there is one ideology that glues the AKP together, it's business: office building in Mersin next to a mosque.

Turkey is the next-door neighbor of the Arab revolutions, and has 100,000 refugees from Syria to show for it. The country lies in the midst of major conflict centers in the Balkans, North Africa, Israel and Palestine, in Syria, Iran and the Caucasus. Turkey's approach to this precarious situation sparks continuous criticism from the West. Whether closer ties or disputes with its neighbors, Ankara's motivations are often regarded as stemming from Turkish history or religion.

Many Western observers think they see two ideologies behind Turkish strategies for coping with conflict: dreams of regional hegemony or Ottomanism, and seduction through sectarian politics – Islamism. Turkey, one often hears, is turning its back on the West.

These labels are as common as they are false. What's happening in Turkey today can be explained far better using ideas we in the West know well, because we invented them: capitalism and nationalism.

These ur-Western concepts have found purchase within Turkish society faster and more profoundly than anywhere in the Middle East. And don't forget the challenge of the Arab uprisings, which directly affect Turkey. All this has shaped its foreign policy amid a crisis environment.

Turkey has transformed itself from a shuttered command economy into a booming export nation. Today, Anatolian fields, once plied by squeaking donkey carts are home to thriving mid-sized manufacturing businesses. These companies export in every direction, and account for most of Turkey's export volume.

The primary market remains Europe, but the Black Sea periphery, Russia, the Middle East and Africa are catching up fast – and changing the Turkish view of the world.

Turkey and Russia were alienated by the Cold War and centuries of rivalry in the Caucasus and Central Asia. Now, five passenger flights a day link Moscow and Istanbul in each direction. A dense web of flights connects Russian and Turkish regional cities. Turkey exports cars, household goods, produce and construction labor northwards; Russia supplies two thirds of Turkey's gas demand, half of its coal and a third of its oil consumption. Russia's state-owned nuclear energy company Rosatom will build Turkey's first nuclear power plant.

Translated, the conservative governing AK party's name means Justice and Development Party. But if there's one ideology that glues the party together, it's business. The AKP includes business associations, media groups, corporations, wholesalers and construction magnates. The party is actively cultivating a country full of capitalists.

Turkey is growing, and most Turks are applauding. Seventy-one percent welcome globalization. When President Abdullah Gül and Prime Minister Recep Tayyip Erdogan travel abroad, their planes are always stuffed with business leaders. With an eye to the future, the government is expanding freedoms in its neighborhood. It is dismantling visa restrictions in all directions.

Unlike Iran, the US and Israel, Turkey views the Middle East not only as an arena for projecting power, but also as its trade fairgrounds. And if business is to flourish, peace has to come first.

Foreign Minister Ahmet Davutoglu has endured countless late-night sessions with feuding neighbors. Turks have mediated between Sunnis and Shi'ites in Iraq, between the two Sudans, Palestinians, Afghanistan and Pakistan. They also were honest brokers in Lebanon and the Balkans. Davutoglu is more than a shuttle diplomat. He is also a strategic thinker.

Turkey, in his mind, is a centrally located state that "unifies many identities" and can maneuver in several regions simultaneously. "That's how we expand our influence," he says.

That shouldn't be mistaken for a national ego trip. "We have been pursuing a zero-problem policy with our neighbors for years," he adds.

That means no more permanent antagonism with neighbors. Cooperation brings advantages for both sides, the Turks learned. The approach paid off richly with Arab and African countries, until the uprisings began.

> "The Arab uprisings have radically changed Turkey's foreign policy environment."

Yet toward Greece, Armenia and Israel it has not. Why is that?

The Turkish Republic was forged in the fires of nationalism, which marks the country's politics to this day. In the early years of his tenure as prime minister, Erdogan purposely muted the nationalist tones in his policies. Since 2009, however, he has again been encouraging the AKP's latent nationalist tendencies, especially around elections. Now, all parties in parliament belong to one camp: the nationalist one.

Erdogan's emotional and confrontational style has made him popular with voters. His tirades against Israel in recent years have exposed the prejudices of a partisan, nationalist politician. Turks loved it. The man on the street lauded the prime minister's skirmishes, even as – without the masses noticing – trade with Israel continued to grow.

Its populist and macho stances have cost Turkey substantial trust in the West, but Erdogan's criticism of Israel has won elections and referendums. He acted exactly the same way in the Armenian question.

In September 2008, President Gül made a historic visit to Yerevan. His intention was to end the diplomatic freeze between Turkey and Armenia and to open the countries' border. Gül came as a visionary, but Erdogan remained a tactician. While diplomats on both sides worked on protocols for a rapprochement, the premier stopped the process abruptly on a visit to Baku, where he promised the Azeris – another foe of the Armenians – to open the Turkish border only once Armenia had abandoned the enclave of Nagorno-Karabakh.

The obsessions of Turkish nationalists with the Armenia question regularly result in serious quarrels with France and the US. It is nationalism, not any Islamic or Ottoman reflex, that draws Turkey into conflict with Western states.

Relations with the EU follow a similar arc. It's become a staple of speechifying in Turkey that Brussels needs Ankara more than vice-versa. Accession negotiations have ground to a standstill – primarily through the fault of the Europeans.

In Cyprus, the EU and Turkey have a seemingly permanent sore point. Suspected gas reserves off the Cypriot coast are providing fodder for even more dispute. In the Aegean, Turkish jets commonly make low-level runs over Greek islands. A resolution in the Turkish parliament from 1996 threatens Greece with war should Athens extend its maritime rights in the region in compliance with the international law of the seas.

To be sure, the AKP-led government has attempted to ease tensions with Greece. Erdogan courts his Greek counterparts and has returned confiscated properties to the Greek Orthodox Church. Yet the nationalists continue to point the way. Since 2005 they have been successfully stonewalling progress towards rapprochement with both Cyprus and Greece.

The Arab uprisings have radically changed Turkey's foreign policy environment. Popular unrest and military conflicts have spelled the end of Davutoglu's no-problem policy and brought many new challenges. Turkey veered from making pacts with dictators to supporting the Arab revolutionaries. In Libya, Erdogan abandoned his former ally Muammar Gaddafi and backed the rebels in Benghazi. The AKP serves as a political role model for Islamic parties from Morocco to Tunisia. Yet the real strategic challenge for Turkey is Syria.

The Turkish premier's once amicable relations with Bashar al-Assad have given way to open hostility. Turkey now offers Syrian refugees safety within its borders and the Free Syrian Army command centers and training camps. Arms are delivered to the rebels via Turkey. The main danger, from Ankara's viewpoint, is a possible push for autonomy by the Kurds in northern Syria. There, Erdogan's failure to resolve the Kurdish question in his own country is coming home to roost.

In Syria, on the other hand, Turkey stands against Russia, China and Iran. Western suspicions of a Tehran-Ankara axis are groundless. Iran has been threatening Turkey both because of Ankara's stance in Syria and its construction of strategic radar systems near the Iranian border. NATO intends to use these to help shield against Iranian missiles.

NICOLE STURZ

Michael Thumann is Middle-East correspondent of the Hamburg weekly Die Zeit.

Flashpoint TURKEY

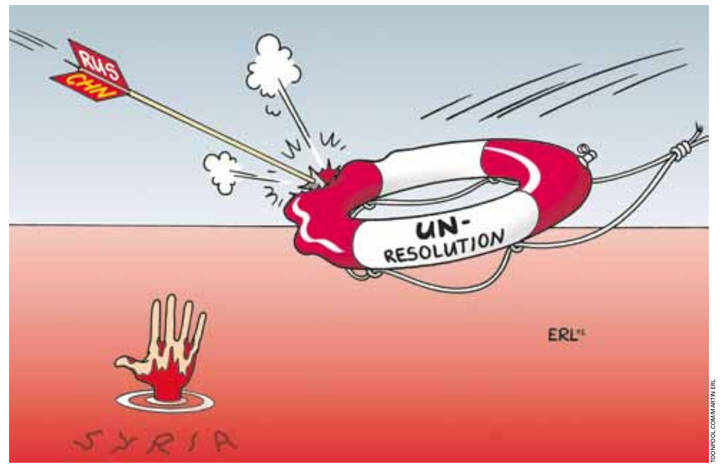
Turkish ties to the US are excellent, and not only since the Syrian uprising began. Turkey may pull away from Europe and place less emphasis on human rights. In the Middle East it will remain the alliance partner of the US, for whom security has absolute priority. ■

Ankara's strategic dilemma

Turkey lies in the midst of major conflict centers

An alternative to force

Why Moscow opposes military intervention in Syria | By Dmitri Trenin



TOONPOOL.COM/MARTIN ERL

Russia's approach to Syria is best analyzed on three levels of diminishing importance. At level one comes the concern about the international order. More specifically, this is about the use of force in international relations and the toppling of regimes from the outside. No longer a Soviet-era superpower, Russia abhors the use of force at will by the United States. Moscow insists that authorization for the use of force is vested solely in the United Nations Security Council. Thus, as a permanent, veto-wielding member of that Council, Russia has the ability to protect its interests. In broader terms, ideal world governance, in Moscow's view, is built on a great-power consensus. The vaunted "multipolarity" is just the most recent iteration of the concept first used in the 19th century Concert of Europe, where the Russian empire felt quite comfortable.

Closely linked with this, and still under the rubric of international order, is the strong emphasis on state sovereignty. Syria, from the Kremlin perspective, is merely another case where the West is in the business of regime change. In Iraq, the United States invaded to topple Saddam Hussein. Iran has long lived under a similar threat. In Yugoslavia, NATO's air war led to the separation of Kosovo from Serbia and the overthrow of Slobodan Milosevic. Most recently in Libya, the Kremlin chose not to oppose a no-fly zone to save innocent lives but was angered when the humanitarian mission then morphed into a regime change operation. Qaddafi had few friends in Russia but his overthrow raised the question of Western credibility. In a way, Syria is paying for Libya.

At level two, there is the Russian government's assessment of the developments in Syria and, more widely, of what is called the Arab Spring. From the very start, Russian Middle East-watchers have been markedly less upbeat on the nature and direction of change in the region. What most of them see can be termed a "Great Islamist Revolution." While Europeans and Americans saw a repeat of Europe's democratic revolutions of 1848 or 1989, the Russians drew parallels to their own of 1917. Early on, Russian policymakers feared an Islamist takeover, and regarded Western countries and pro-Western liberals as paving the way for religious radicals or al-Qaeda allies.

CARNEGIE.RU

Dmitri Trenin is Director of the Carnegie Moscow Center.

Flashpoint SYRIA

This fear is deepened by events in Syria where Bashar al-Assad's opponents include Jihadist elements and where the danger of a sectarian war is very real. In the Russian government's calculus, Assad is likely to hold on to power for quite some time. But his overthrow will not mean the end of the civil war, only the beginning of its next phase. In President Putin's words, the Syrian government and the opposition will just switch places, and the fighting will continue. Having such a cauldron of large-scale violence only a few hundred miles from Russia's own troubled North Caucasus is not good news for Moscow, especially with the Winter Olympics in Sochi less than two years away.

Russia's material interests in Syria itself are of only third level importance in this analysis. Damascus is no longer Moscow's ally. The Russians withdrew from the regional power play in the Middle East as long ago as 1990, at the time of the first Gulf War, and have not re-entered the race since. Moscow is a loyal, if relatively insignificant member of the Middle East Quartet. It does not seek to undermine US interests in the region, its ties with Arab regimes have grown cold and, in a most dramatic about-face, the Kremlin has befriended Israel.

Syria does not even come close. Bashar al-Assad is a commercial partner for the Russian defense industry, but the overall economic relationship is not particularly thriving. To persuade Damascus to agree to new purchases of Russian arms, Moscow has had to agree to cancel billions in past Syrian debts to the Soviet Union. The Tartus naval resupply facility on the Mediterranean coast is useful for the Russian Navy, especially as it is the only such station anywhere outside the former USSR, but, with a personnel of about 50, it is a far cry from being a naval base. There are also thousands of Russian-born wives of Syrian citizens – many of them military officers – who once studied in the Soviet Union, and of course their children, but that's about it. Real and substantial as they are, these interests are fairly limited.

The implications of this analysis are several. Moscow is neither pro-Assad nor anti-West, but its position on the issues of the primacy of the UN Security Council and the importance of sovereignty will not change. In stark contrast to the Soviet Union, Russian leaders today abhor revolution and favor procedure over emotion and ideology. Moscow knows that the West can once again ignore its opposition and intervene in Syria with force. That would not provoke a Russian military action, but the rift between Moscow and Washington would grow deeper. This, in turn, would likely harden Russian attitudes to other crisis situations, particularly over Iran. Finally, the pattern of Sino-Russian opposition to US-led or US-backed use of force around the world, which appeared to be easing with Libya, would be further strengthened.

While the West should not hope that Russia (or China) will simply join it on Syria, it can engage with Moscow and Beijing to stop the violence in the country, and prevent the spread of the conflict. For that to happen, the P5 (permanent members of the UN Security Council), in consultation with the countries in the region, from Israel to Iran, from Turkey to Saudi Arabia and from Egypt to the United Arab Emirates, need to bring their influence to bear on all Syrian parties to stop the fighting and start talking. The negotiations, closely overseen by the world and regional powers and legitimized by the UN, should be about a new political system for Syria, which would install democracy while protecting the rights of minorities: Alawites, Christians, Kurds and others.

Assad will have to go, no question about it. But how he goes will make all the difference. The aim should be a Dayton-in-the-Middle-East. The alternative might be a military victory in terms of Assad's ouster by the Free Syrian Army supported by a Western-led coalition – but it would probably be a Pyrrhic one. ■

How dangerous is Pakistan?

Upcoming elections offer hopes of a new political leadership | By Ahmed Rashid

PICTURE ALLIANCE/DPA/FAYAHMED KHAN

Pakistan is the key to the timely and safe withdrawal from Afghanistan of troops from 49 countries. But the country is itself beset with multiple crises, burgeoning insurgencies and a lack of decisive governance.

For seven months, it isolated itself from the Western alliance by closing the main supply and exit route for NATO equipment from the port city of Karachi to the Afghan border. Yet the road's re-opening in August has only intensified the domestic problems Pakistan continues to face. At stake is the future stability of not just Pakistan but also Afghanistan in what has become the most volatile region in the world.

On July 3, US Secretary of State Hillary Clinton finally said the magic words in a phone call with her Pakistani counterpart: "We are sorry for the losses suffered by the Pakistani military." It was a tepid apology for the killing of 24 Pakistani soldiers last November by US helicopter gunships, but enough so that the Pakistanis agreed to reopen the border crossings into Afghanistan that had been closed since the incident.

During those seven months, Pakistan found itself isolated from an angry and frustrated Western alliance. But it also earned the ire of its key allies, China, Turkey and Saudi Arabia who asked the government why it had boxed itself into a corner with the US and was refusing to deal with the continued insurgency by Pakistani Taliban in the northwest of Pakistan, who were also training terrorists from these allied countries.

Pakistan's indecision for so many months was a result of a three-way-split in governance between the all-powerful army, the elected Pakistan Peoples Party government and the Supreme Court. The PPP and its allies are trying to make it through until next March 2013 when general elections have to be held. Simultaneously, the Supreme Court – which has already forced the resignation of one Prime Minister (Yousuf Raza Gailani) – has spent much of the year trying to force the resignation of President Asif Ali Zardari on corruption charges.

The army, which controls foreign policy and all national security issues, is facing a wave of internal dissent and growing anti-Americanism within its ranks that appears to have paralyzed its decision making process.

For seven months nobody in the squabbling troika wanted to take the decision or bear the responsibility for reopening the road to Afghanistan. Now that it is open and tentative steps have been taken to try and restore relations with the US and NATO, the government is failing on other fronts: the tough decisions needed for economic reform; Protecting the minorities whose members are gunned down daily by a variety of extremists; acting against the Pakistani Taliban or launching a political initiative to end the separatist uprising in Balochistan province.

The underlying issue is the ruling elite's failure to carry out reforms. The army and the politicians lacked the courage or will to take the necessary tough decisions such as making peace with India, blocking the growth of extremism or carrying out desperately needed economic reforms, when the rest of the world was surging ahead on a peace dividend and globalization after the end of the Cold War. In the 1990s the army immersed itself in covert wars, first in Afghanistan supporting the Mujaheddin and later the Taliban, and then in Indian Kashmir supporting the Kashmiri jihadists – many of whom were actually Pakistani militants.

In the 1990s, tens of thousands of jihadists were trained by the army. Pakistan was thoroughly undermined from within, even before it took the unwise decision to give shelter to escaping Afghan Taliban militants from Afghanistan in 2001 in order to sustain "options" against the US presence in Afghanistan. Until recently, Islamic extremists were still a tool of the military and the foreign policy goals pursued by its intelligence services.

However, awareness is creeping in. For the first time, army chief General Ashfaq Kiayani warned in an Independence Day August 14 speech that: "The fight against extremism and terrorism is our own war and we are right in fighting it…otherwise we'll be divided and taken towards civil war."

Backed up by the threat of more drone attacks, the US and NATO have been insisting that Pakistan contain the cross border attacks of the Afghan Taliban, in particular the Jalaluddin Haqqani network which has launched some spectacular attacks against NATO forces. Earlier, the killing of Osama bin Laden in his lair in the heart of Pakistan was another blow to the country's image. The al-Qaeda leader's presence in Pakistan infuriated the US and NATO – especially as the Pakistani intelligence services still have not explained what he was doing there.

Anti-Americanism in Pakistan is growing. Supporters of the Jamat e Islami party protest against the re-opening of the NATO supply route, in Karachi. US and NATO forces in landlocked Afghanistan get around 75 percent of their food and military supplies through Pakistan. Radical Islamists have frequently attacked NATO transports, here in August 2011 in Baluchistan (opposite page).

PICTURE ALLIANCE/DPA/TARIQ DEHGHI

PRIVATE

Ahmed Rashid is the author of the bestselling books "Taliban" and "Pakistan on the Brink: The Future of America, Pakistan and Afghanistan."

Flashpoint PAKISTAN

Yet Pakistan has also paid a terrible price for its inability to curb extremism. The government says 35,000 people have been killed over the past decade by the Pakistani Taliban, related militant groups or in bitter sectarian war that has gone unchecked, with all minority religious groups now at risk at the hands of Sunni extremist groups. Those targeted include Hindus and Christians but also Muslim groups like the Ahmedis, Ismailis, Memons and Shias. In Karachi, the breakdown of law and order is leading to the growth in the slums of armed militias based on ethnic, criminal or political loyalty.

> "Pakistan desperately needs new political leaders who can tell its people the unvarnished truth about past mistakes."

The Obama administration's lack of a strategic policy towards Pakistan and the many tactical mistakes it has made over the past two years has only intensified anti-Americanism. Many Pakistanis believe that it's the Americans who have got it all wrong and if only they were to leave Afghanistan, everything would right itself.

The Obama administration has now declared the Haqqani network a terrorist group. That could lead to Pakistan being branded a state sponsor of terrorism, because of Haqqani's safe havens. Any such US move could prompt a fresh crisis with the Pakistan military, harden anti-Americanism among the public and politicians and isolate Pakistan even further.

Islamabad had taken no steps to avert the policy disaster of the Haqqanis being labelled terrorists. Leadership and decisive decision-making was required, first to contain the Haqqanis by forcing them to stop their attacks on US forces and then by opening talks between them, the Americans and the Afghan government just as other talks are ongoing with the Afghan Taliban.

Pakistan desperately needs new political leaders who can tell its people the unvarnished truth about past mistakes, stop blaming India or the US for its ills, end its isolationist tendencies, carry out economic reforms and ultimately create a new narrative that educates the public about the threat of extremism rather than hiding behind a series of denials.

Sixty-five percent of Pakistan's 180 million people are below the age of 25. Unless the political establishment is able to offer these young people a more hopeful future that is in line with global trends, and a new narrative that preaches hope and nation-building rather than Islamic extremism, Pakistan will continue to slide. The forthcoming elections are certainly one hope that a new political leadership will emerge that can point the country in the right direction. ■

Weighing the options in war-ridden Syria

The endless suffering of the civilian population demands intervention – but political considerations call for restraint | By Guido Steinberg

In recent weeks, the escalation of the violence in Syria has led to an intensification of the debate over a possible Western military intervention. In mid-August 2012, President Barack Obama called the deployment or use of chemical or biological weapons by the Syrian regime a "red line" for the United States. He thereby suggested that his administration was giving serious thoughts to the possibility of having to intervene militarily if weapons of mass destruction threatened to fall into the hands of militant groups or if they were directly used by the Syrian regime.

Ever since these remarks, the debate over a possible intervention has continued, showing how much the escalating killing of civilians all over Syria has unnerved the international public. But it remains highly unlikely that the US administration will change its cautious policy with regard to Syria – and this is in fact the only responsible way to deal with the crisis for the US and its allies.

This policy is based on a realistic reading of the situation in Syria, where it is far from clear who will prevail. The regime of Bashar al-Assad is struggling to reestablish its control over the whole of Syria's territory but its units are still highly superior to the rebel forces.

However, the regime lacks reliable manpower to hold areas once it has forced the insurgents to withdraw from certain towns or city quarters. This has become obvious in Damascus, where fighting has resumed after government forces claimed to have cleared the city of insurgents in late July 2012.

> It would be unwise to become immersed in a struggle of minor importance and, in doing so, tie one's hands on the larger issue: Iran.

The rebels, on the other hand, are in no position to defeat the regime either. They still lack the manpower, money and weapons to confront government forces head-on and they also suffer from insufficient military and political coordination of their activities. As a result, they have not been able to translate their biggest success – namely their very survival in the face of the regime's brutal onslaught – into any improvement of their strategic position. The result of this strategic stalemate has been an escalation of violence into a civil war that might continue for years.

Although the Obama administration has made clear that it believes that Bashar al-Assad will lose in the long run, it has not taken decisive action to help the insurgents but has limited itself to providing them with non-lethal equipment like communications gear. This cautious approach is also due to the nature of the conflict, which is not restricted to its most obvious dimension, namely the fight between an authoritarian regime and an armed opposition movement. Rather, the US government is keenly aware of the ideological dimension of a conflict where a secularist regime is challenged by a strongly Sunni Islamist (and thereby anti-American) opposition and the dangers of regional escalation if Washington decided to intervene more forcefully.

> In all states where the Arab spring has weakened the ruling regimes, Islamist parties and groups have become important players in the new political systems.

In all states where the Arab spring has weakened the ruling regimes, Islamist parties and groups have become important players in the new political systems. In Syria, the Muslim Brotherhood has every chance of duplicating the victories of their brethren in Tunisia and Egypt. About 70 percent of the Syrian population are Sunni Arabs and there are clear indications that Sunni Islamists are strongly represented among the rebels, while the regime is increasingly withdrawing to its power base among the Alawites, who are considered a heretic sect by Sunni Muslims, hated for their support for the Assad regime, the President himself being one of them.

In the worst case, a victory of the rebels would result in large-scale killings of Alawites and possibly Christians, Druze, and Kurds. Even in the best case, any rebel government in Damascus would most likely be strongly Islamist in outlook and as a result not overly sympathetic to the US, regardless of Washington's role in supporting the insurgency.

Adding to the widespread scepticism in Washington is the increasingly prominent role of Jihadists in the insurgency. The al-Qaeda affiliate in Iraq has already taken the chance to send personnel and arms to Syria, and a local Jihadist group named Front for the Protection of the Syrian People (Jabhat al-Nusra li-Ahl al-Sham) has been responsible for several of the large-scale bombings in Damascus and Aleppo in recent months.

These groups have brought non-Syrian militants into the country, but have also profited from the existence of a strong Jihadist underground in the country, which already provided the Iraqi insurgency with thousands of fighters and which today provides the Syrian rebels with well-organized and battle-hardened warriors. It is no wonder that the US hesitates to support an insurgency in which these groups play a role, however limited that role might be.

Guido Steinberg is a Middle East expert at the German Institute for International and Security Affairs (SWP).

SWP-BERLIN.ORG

Flashpoint SYRIA

Add to that the regional dimension. As in most civil wars, outside powers are trying to influence events in Syria and there is every indication that the conflict is part of a larger regional cold war between Iran and its allies on one side and Saudi Arabia, Qatar and other pro-Western regimes on the other.

Iran has been Syria's major ally since 1980 and its rulers are supporting the Assad regime in its current crisis. Although the Iranians are still eager to hide their engagement, there are hints that they have recently stepped it up by sending much-needed reinforcements to quell the rebellion. The Iranian leadership sees the conflict in Syria as a first step in a Western effort aiming at the downfall of the regime in Teheran and might therefore be expected to intensify its efforts on behalf of the Assad regime once it comes under increasing pressure.

The insurgents are mainly supported by the Saudi Arabian and Qatari governments, who see the opportunity to weaken Iran by toppling its most important Arab ally. Although still hesitant because of the lack of a clear American commitment, Riyadh and Doha have been the main financiers of the rebels and are providing them with weapons as well.

A Western intervention in such a situation would be fraught with dangers. First, the Saudis and Qataris would try to manipulate any Western supporter for their own ends. This would be especially serious in the case of Qatar, whose regime has openly stated that it sees Islamists and Salafists as its future political allies in the Arab world. Supporting local clients of Saudi Arabia can also be problematic because the Kingdom is looking for allies in its confrontation with Iran rather than reliable partners who will rebuild a peaceful Syria.

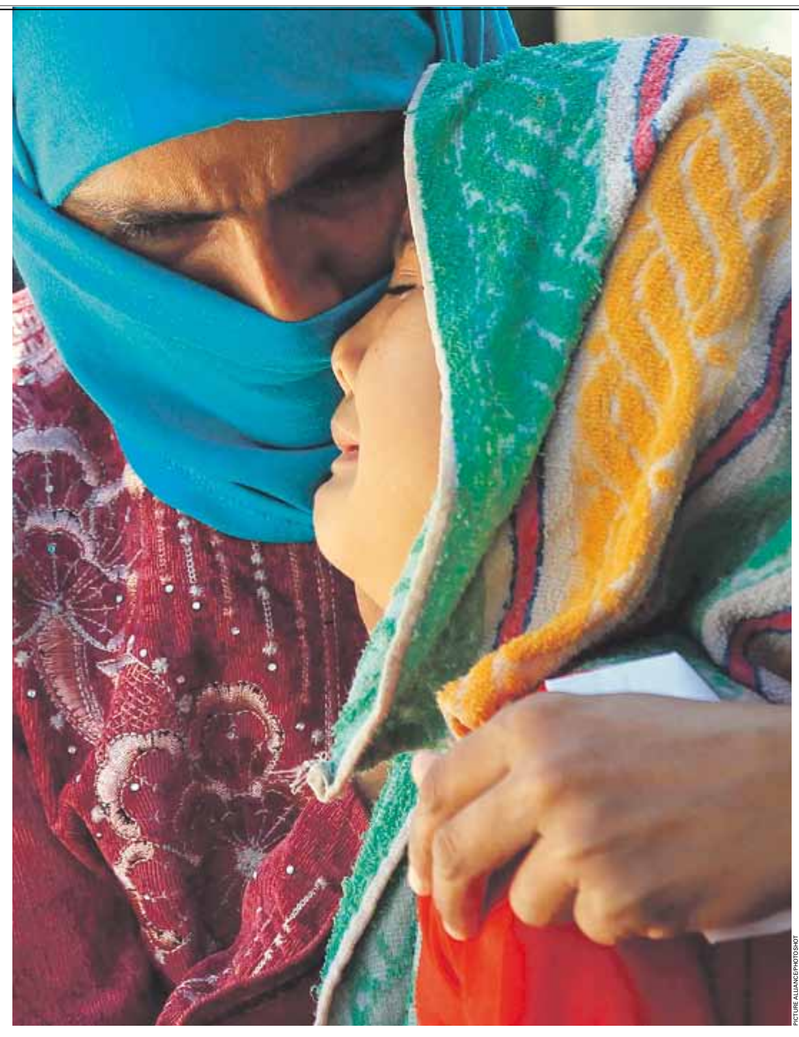
Secondly, any Western troops deployed to Syria and its neighborhood would be confronted with powerful militant adversaries – be it the Hezbollah, the PKK, al-Qaeda or newly formed groups – who would try to draw them into an asymmetric fight. The US has rightly drawn the conclusion out of the fiascos in Iraq and Afghanistan that it should avoid similar imbroglios in the future.

But perhaps most importantly, this US administration sees that the moment will come when it is necessary to use force against Iran in order to keep it from building a nuclear bomb very soon. It would be unwise to become immersed in a struggle of minor importance and, in doing so, tie one's hands on the larger issue.

The Bush administration did exactly that when it invaded Iraq in 2003. The result was an immensely strengthened Iranian regime on the verge of achieving nuclear weapon capability. Any intervention in Syria might have similar results and would only distract the US from the much more important Iran issue.

The American position reflects a sober reading of the regional situation. It is the right way to keep up pressure on the Assad regime by sanctions and try to keep it from using weapons of mass destruction by all possible means. At the same time, the US and its allies should continue trying to force the Syrian opposition and insurgents to find a common political platform that is able to convince the minorities in the country that they will not be targeted once the regime falls.

In general, the question whether to intervene or not is a classical dilemma, especially when considering the suffering of the Syrians themselves. Nevertheless, the prospect of an escalating regional cold war with a nuclear-armed Iran as the prime adversary is the far more dangerous scenario. ■



PICTURE ALLIANCE/PHOTOSHOT

To intervene or not? Syrian refugees at the Al Zaatri refugee camp in the Jordanian city of Mafraq mid August.

Staking claims in the South China Sea

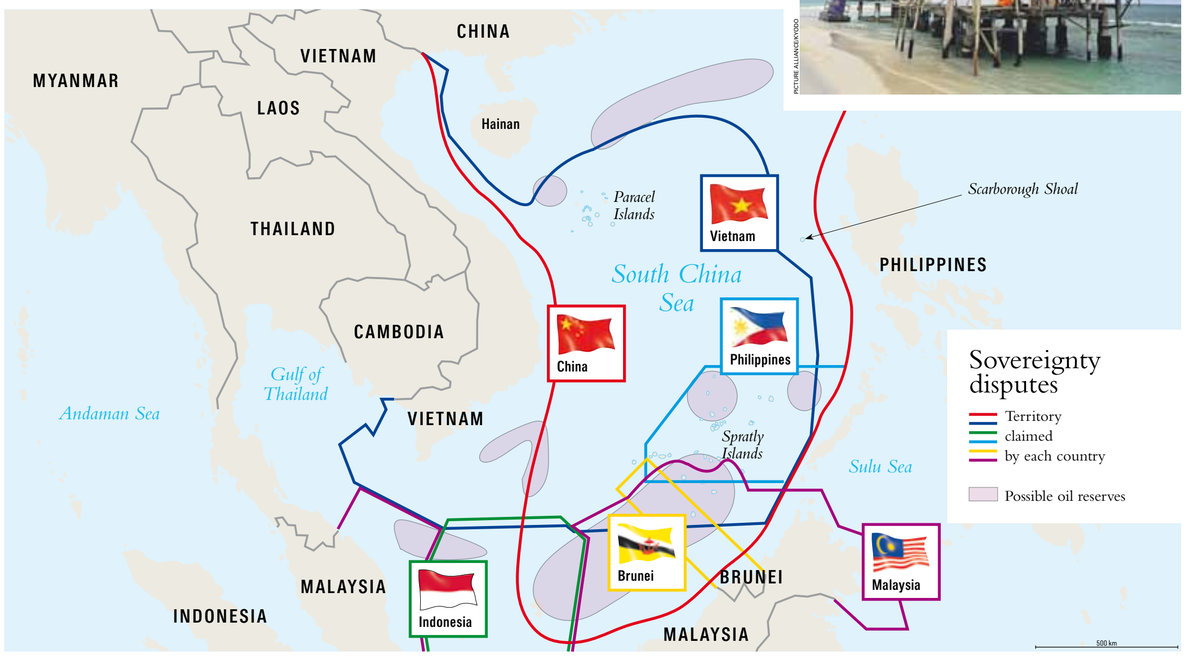
The maritime region is awash with sovereignty disputes | By Carlyle A. Thayer

AFP/GETTY IMAGES/ROMEO GACAD

DDP IMAGES/JAPAN 3D.COM/CHINA

PICTURE ALLIANCE/KYODO

Disputes over territory and maritime exclusion rights feed tensions in the South China Sea. A Chinese military outpost at Meiji Reef, which is also claimed by Taiwan, the Philippines and Vietnam (left). Chinese officials inspect the fishery base at the Meiji reef (above). Beijing imposes unilateral fishing bans to enforce its sovereignty. A Philippine military base on Lankiam Cay, the smallest of the Spratly Islands (below).



The South China Sea is fast emerging as a regional hotspot; its contested waters are becoming more congested, raising the risk of a deadly naval engagement through misadventure. These risks are magnified by rising jingoism, resource nationalism and militarization.

Tensions are rising as China presses its claims to all of the islands and eighty percent of the waters in the South China Sea. This year Beijing adopted more confrontational tactics towards the Philippines and Vietnam in order to assert sovereignty claims. Both countries have turned to the US to counterbalance China.

The South China Sea is a semi-enclosed maritime area that straddles the world's second most important sealanes. Nearly half of global shipping and an estimated seventy percent of crude oil imported by China, Japan, South Korea and Taiwan passes through the waterway.

The South China Sea is dotted with several hundred islands, islets, rocks, reefs, shoals, and sand banks. These features are grouped into two archipelagos, the Paracels and the Spratlys.

It is estimated that between 43 and 48 islands, rocks and other features in the Spratlys are currently occupied. Vietnam possesses between 21 to 25 islands and rocks, the Philippines eight to nine, China seven to eight, Malaysia five to six, and Taiwan one. China occupies all of the Paracel Islands but sovereignty is contested by Vietnam.

The South China Sea is host to one of the world's most productive fishing grounds. It is believed to contain rich reserves of oil and gas. The extent of hydrocarbon reserves is not known precisely. China regularly provides estimates that are several orders of magnitude greater than those provided by the US Department of Energy.

Under international law, the littoral states of Southeast Asia are entitled to claim a 200 nautical mile Exclusive Economic Zone (EEZ) from their coastlines and around their islands that entitles them to exercise sovereign jurisdiction over the resources in this area.

China bases its claims to sovereignty on historic rights. In 2009 it officially issued a map containing nine "dash lines" forming a U-shape enclosing the South China Sea. These demarcation lines cuts deeply into the EEZs claimed by Vietnam, the Philippines, Malaysia and Brunei. China claims all the islands that lie within this area including those currently occupied by other states.

Since 2009 China has asserted its claims to sovereignty in the South China Sea by aggressively enforcing an annual unilateral fishing ban. In April this year, Chinese civilian ships prevented the Philippines from arresting illegal Chinese fishing boats at Scarborough Shoal by physically blocking access. During the two-month stand-off China dispatched nearly one hundred fishing craft to occupy the shoal. China also applied economic sanctions by banning the import of bananas and cancelling tourist charter flights.

> "Tensions in the South China Sea are overlayed by strategic rivalry between China and the United States."

Chinese civilian vessels have also interfered with the commercial operations of oil exploration vessels in waters lying within its U-shaped line. In 2011, Chinese ships drove off an oil exploration vessel in Philippine waters and twice cut the cables of oil exploration vessels in Vietnam's EEZ.

In June, when Vietnam's National Assembly passed a Law of the Sea covering its EEZ and islands, China retaliated by issuing nine exploration leases in blocks falling entirely within Vietnam's EEZ. China then elevated the administrative status of Sansha City and gave it jurisdiction over the South China Sea. China also announced that it was establishing a military garrison in the Paracels and commenced "combat ready" patrols.

Vietnam has responded to Chinese assertiveness by building up its military capabilities. Vietnam has taken delivery of Su-30MK jet aircraft and stealth frigates. Hanoi has also ordered six Kilo-class fast attack submarines. All of these platforms will be armed with anti-ship cruise missiles. The Philippines have embarked on a more modest arms build-up.

Tensions in the South China Sea are overlayed by strategic rivalry between China and the United States. China is rapidly developing anti-access/area denial capabilities designed to force the US Navy from operating in international waters off China's coast.

China's naval base on Hainan island houses a growing number of modern surface combatants as well as nuclear attack submarines. On several occasions China has challenged US military aircraft and ships operating in waters off Hainan. China has also threatened to impose sanctions against American oil companies operating in China if they assist Vietnam in developing its offshore oil and gas resources.

The Obama administration responded to Chinese military and commercial pressures, as well as lobbying from Southeast Asian states, by declaring that the United States has a national interest in freedom of navigation, over flight and unimpeded commercial activities.

The Obama administration opposes the threat or use of force to settle territorial disputes in the South China Sea and advocates a collaborative diplomatic approach to resolve them. China counterargues that territorial disputes must be solved bilaterally by the states concerned. Beijing also argues that the United States is an outsider with no standing in the matter.

On Aug. 3, when the US State Department noted that the establishment of a military garrison in the Paracels as well as other Chinese actions risked escalating tensions, China responded by summoning the deputy chief of the US Mission in protest. The People's Daily editorialized: "We are entirely entitled to shout at the United States, 'Shut up'. How can meddling by other countries be tolerated in matters that are within the scope of Chinese sovereignty?"

Yet a month earlier when Southeast Asian foreign ministers attempted to draft a joint communiqué mentioning recent incidents at Scarborough Shoal and in Vietnam's EEZ, China intervened behind the scenes to scuttle the statement.

The United States policy of rebalancing its military forces in the Asia-Pacific seemingly has put it on a collision course with a rising and more assertive China. The risks of conflict in the South China Sea appear to be growing as China's domestic power shift takes place in an environment of growing jingoism, resource nationalism and militarization. ■

UNSW CANBERRA

Carlyle A. Thayer is Emeritus Professor at the Australian Defence Force Academy, Canberra.

Flashpoint SOUTH CHINA SEA

Obama's pivot to the Pacific

Washington's focus on Asia was unavoidable but is it sustainable as a matter of long-term US strategy?

By Daniel Twining

PICTURE ALLIANCE/PHOTOSHOT

Pivoting: US President Barack Obama and Chinese President Hu Jintao in Seoul, March 2012.

The Obama administration's declaration of a US "pivot" to Asia came at a useful time, providing as it did domestic political cover for the withdrawal of US military forces from Iraq and Afghanistan. Clearly, President Obama's political opponents could not accuse him of projecting American weakness, despite the chaos and violence left in the wake of the premature US drawdown in the Middle East, even as he promised to stand up to Chinese assertiveness in Asia by strengthening US alliances.

In fact, it was President Obama himself who pivoted: from pursuing a US-China "G-2" condominium in 2009, causing deep anxieties among American allies in Asia and Europe, to declaring a military buildup that was clearly aimed at China only two years later. As Joseph Nye has argued, the US "pivot" to Asia is not new. Rather, since the end of the Cold War it has seen three distinct phases under three successive US presidents.

The first started in 1995, when Nye and other senior Clinton administration officials launched a process that culminated in the revitalization of the US-Japan alliance for the post-Cold War era. The second phase started in 2005, when the George W. Bush administration achieved a breakthrough strategic partnership with India that ended half a century of alienation between the world's largest democracies and positioned the United States as the premier partner of Asia's other rising giant.

President Obama has presided over the third phase of America's reorientation, toward the Asia-Pacific. His administration has helped strengthen Asian regional institutions by sending senior officials to Asian summits; encouraged Burma's fragile political and economic opening; launched a US-Japan-India trilateral grouping that could anchor a future Asian balance of power; and deepened US military relations with key partners, especially South Korea, the Philippines, Singapore, and Vietnam.

The US administration has had less success advancing US leadership on trade, as important a source of regional influence as military prowess – although President Obama did finally enact the Bush-era free trade agreement with South Korea, and has continued negotiations on the Trans-Pacific Partnership the Bush administration launched with Asian partners in 2008.

Diplomatically, Secretary of State Hillary Clinton and other senior US officials have broken new ground in supporting Southeast Asian countries anxious about China's infringement of maritime security. One-third of world trade passes through the waters of the South China Sea, and Washington has aligned with almost every Asian capital in opposing China's unilateral threat and use of force to back up its claims to this international waterway. Indeed, China's assertiveness over its expansive territorial claims has caused many Asian states to expand defense relations with America as a hedge against Chinese bullying.

> "... the world may not allow America the luxury of focusing on Asia to the exclusion of other regions."

Militarily, the Obama administration has broken important new ground as well. Secretary of Defense Leon Panetta has redeployed US navy vessels from the Atlantic to the Pacific and Indian Oceans. A military basing agreement with Australia will position US combat vessels and Marines near contested Southeast Asian waterways. Enhanced access agreements will see US Navy ships and personnel transit Singapore and other Southeast Asian ports on a regular basis. Japan, the Philippines, and other states may host elements of a US missile defense system designed to intercept North Korean and Chinese missiles. India's armed forces now exercise more with US counterparts than with the forces of any other country, and the United States has become one of India's top defense suppliers.

These are welcome developments. The question is whether the rebalancing towards Asia is sustainable as a matter of long-term US strategy. President Obama has proposed up to $1 trillion in defense spending cuts over the coming decade; the US Navy has fewer ships and submarines than at any time since 1917. How will the United States pay for the "pivot" unless these trend lines are reversed, particularly as China develops anti-access capabilities that make American forces in the region more vulnerable?

Moreover, the world may not allow America the luxury of focusing on Asia to the exclusion of other regions. Irrespective of whether his last name is Obama or Romney, the next US President is likely to be as consumed with Iran and Syria as the last US President was with Afghanistan and Iraq. Nor is a crisis in Pakistan unimaginable. Although he will sustain a robust Asia strategy, the man in the Oval Office in 2013 may find that he is pivoting back to the wider Middle East, given its intractable and immediate security crises.

This raises a broader point. For over four decades, as part of its epic contest with the Soviet Union, the United States worked closely with its allies to manage a global grand strategy that encompassed every region. American officials did not choose between Europe or Asia, Latin America or the Middle East; they and allies in Europe and Japan pursued policies that, while often imperfect, maintained a global balance of power and ideas that ultimately achieved victory in the Cold War.

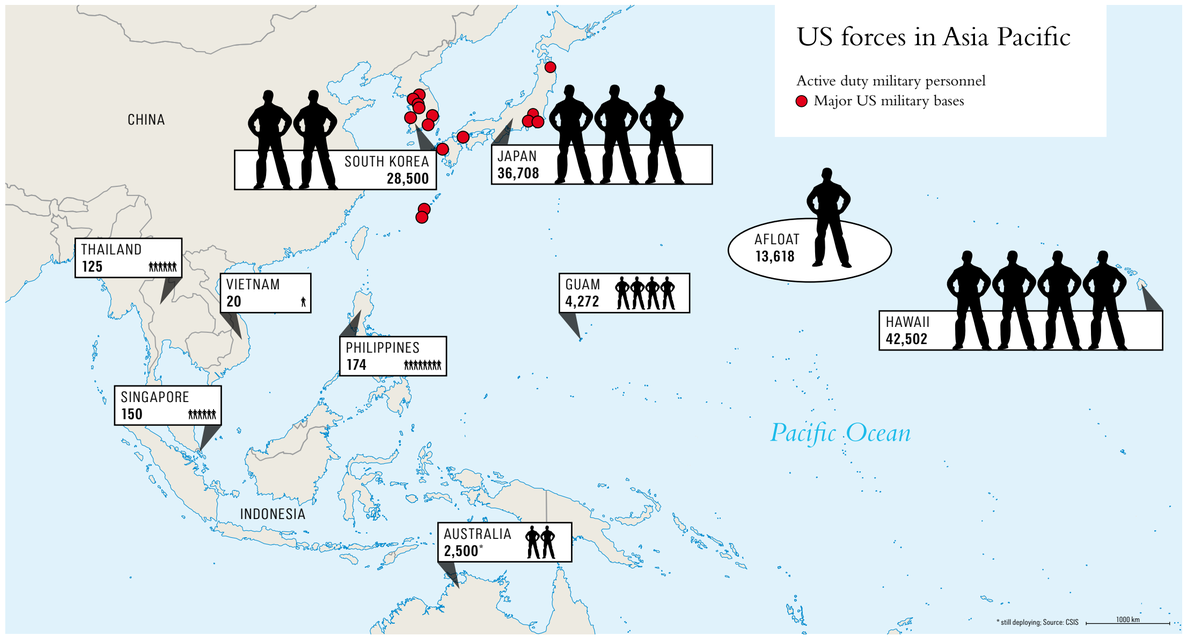
In the far more globalized, interdependent, and diffused world of the 21st century, it would be surprising – and regrettable – if Washington's focus on Asia caused relations with old and new friends in Europe, Latin America, Africa, and the Middle East to wither. Asia's re-emergence may actually make these partners more, not less, important.

After all, the rise of Asia is a global phenomenon, impacting not only on its region but on international norms, the balance of power in international institutions, the security of the global commons, and management of the world economy. As important as it is for the United States to help shape the new Asia, it is equally important for Washington to work with allies in Europe and elsewhere to ensure that Asia's ascendance enhances global integration – rather than eroding the liberal international order that has produced prosperity and security for East and West alike. ■

GERMAN MARSHALL FUND OF THE US

Daniel Twining is Senior Fellow for Asia at the German Marshall Fund of the United States in Washington, DC. He formerly served as a Member of the US Secretary of State's policy planning staff.

Flashpoint ASIA-PACIFIC



Leaving Afghanistan without abandoning it

The aim of the gradual withdrawal is to ensure the success of the handover to local forces | By Jamie Shea

Nothing in his life became him like the leaving it," wrote Shakespeare famously of his character Macbeth. The same could be said of NATO's International Security Assistance Force (ISAF) mission in Afghanistan, which is due to end on Dec. 31, 2014.

Our perception of the value of military engagements is shaped inevitably by the way in which they end. We think of Russians and Americans shaking hands for the cameras at Torgau in 1945, but also of Vietnamese civilians clinging to the skids of US helicopters above the Saigon Embassy in 1975.

"Mission accomplished" must not only be proclaimed but convincingly demonstrated, either in terms of the comprehensive defeat of the adversary or the perspective of a brighter, more orderly future. The way in which conflicts end determines to what degree they were worth the blood and effort of fighting them in the first place.

For these reasons, ISAF's withdrawal from Afghanistan is as much a political as a logistical challenge. The Alliance's commitment to Afghanistan has been its most ambitious venture to date.

At the time of writing, over 2,000 US and 3,000 Allied soldiers altogether have given their lives in this endeavor. Inevitably by 2014, this figure will be higher still. Although ISAF first deployed to Afghanistan in 2003, the bulk of the casualties have occurred in the last two years as fighting in the south and east has intensified.

The purpose of ISAF's gradual withdrawal, over the best part of two years, is not to smoothly extract our troops from the line of fire (according to the principle that the most complex military operation is an orderly retreat) but rather to demonstrate the success and durability of the handover to the Afghans themselves, and their capacity to keep Afghanistan and its people together, and at relative peace, without a permanent international life support machine. From this perspective, it is possible to assert a pattern of strategic progression, which has frequently been obscured by the daily bad news stories of "green on blue" attacks, bank scandals, or "adulterous" women stoned to death.

But how can NATO still win its campaign when every seven minutes one of its military containers leaves Afghanistan and its numbers begin to shrink as nations pack up their equipment and roll back from their bases? How can it exert maximum influence when it is well past the peak of its military power and presence; and when the Alliance's politicians and publics increasingly tune out as they conclude that Afghanistan is finished business?

Afghan soldiers on a joint exercise with NATO troops.

PICTURE ALLIANCE/DPA/JAUL HEZAYET

Jamie Shea is Deputy Assistant Secretary General for the Emerging Security Challenges Division at NATO.

NATO

Flashpoint AFGHANISTAN

The answer is not just to use the next two years to withdraw but also to prepare for the day after, when Afghans will assume responsibility for their own security. In other words: to leave Afghanistan without abandoning it. NATO will have to fight to weaken the Taliban, as far as possible, and train the Afghan army, police and local police at the same time. Ideally this means keeping as many combat troops in theater for as long as possible and having a planned withdrawal whereby forces in quieter areas and those occupied with logistic or headquarters tasks leave first. Inevitably the brunt of this effort will fall on the Americans because of their greater resources and their presence in the south and east. President Obama has already decided to bring home the 33,000 "surge" US forces he deployed in 2010 to help win back Kandahar and the south. But, given popular pressure to terminate the mission, will the US keep in theater the remaining 68,000 US forces until at least late in 2014? The special operations forces, which do the bulk of the fighting, and which operate closely with their Afghan counterparts, will be especially crucial.

Sooner or later, the Allies will also need to address the question of which residual military presence they wish to leave behind. Trainers have already been agreed, but what about special forces, air and helicopter units, intelligence cells and technicians to assist the Afghans? Close air support will be particularly important, as will be intelligence and logistics.

There is little use leaving the Afghans a lot of highly sophisticated military technology if they do not have the ability to operate it, or cannot afford to maintain it. Far better now to agree on the equipment that the Afghans can use optimally, and train them on it - for instance, metal detectors rather than satellites to find roadside explosive devices. And will the NATO trainers not also need force protection as was the case in Iraq, and especially if they are widely dispersed? What kind of footprint, light or heavy, or facilities will this require?

It will be important to define the scope and mandate of NATO's follow-on presence in Afghanistan as well as those non-NATO partner countries who will participate in it as early as possible. This will help NATO to define a smooth glide path in knowing what material and facilities to take away or close down, what to hand over to the Afghans in the form of military assistance, and what to leave behind for its own new training, assistance and advisory mission. An early decision will also be helpful to obtain the buy-in of the Afghan government and to jointly socialize the decision with the Afghan population that frequently lives between fear of abandonment and fear of foreigners forever running Afghan affairs.

> "Sooner or later, the Allies will also need to address the question of which residual military presence they wish to leave behind."

Will the Afghan forces be up to the job of handling security once ISAF leaves? The answer can only be given definitively once we come to that juncture. Will those Afghan forces be less or more effective (and motivated) with or without their ISAF chaperones? Expert views differ so much on this question that it is difficult to form a judgement.

On the plus side, ISAF has already transferred three quarters of Afghanistan's provinces and an equivalent percentage of its population to the control of the Afghan security forces. There have been no major security problems in the areas handed over to Afghan control, so that the next stage of handover (Tranche 4) can follow at the end of 2012.

The fighting is concentrated in less than 10 percent of the territory with less than six percent of the population. Moreover, the Afghan units, or Kandaks, now carry out 80 percent of all missions. They have done a credible job of repelling the Taliban especially during urban attacks against the US Embassy, Afghan ministries and international hotels in Kabul. They have suffered higher casualty rates than the international forces and desertion rates have come down.

Indeed, one of the reasons suggested for the spate of "green on blue" attacks by Afghans against their ISAF colleagues in the spring/summer of 2012 was the greater stress of regular combat they are facing (600 Afghan soldiers were killed in the first six months of 2012). It is depressing that over 10 percent of ISAF casualties are now the result of these "insider" attacks (47 in 2012 at time of writing); but the inevitable emotional outrage should not detract from the reality that the bulk of the Afghan forces are loyal and fighting well. They are also the victim of insider attacks.

Former US Defense Secretary Donald Rumsfeld famously said, "You go to war with the army you have, not the army you might want or wish to have at a later time." In this vein, the Afghan security forces will continue to be a work in progress. A balance will need to be struck between the numbers Afghan security will require versus how much the international community can afford to pay to sustain those forces on a long-term basis and whether other countries besides the Allies will pay into the fund.

$4 billion a year is the estimate but it is probably the minimum and, as we have seen before, armies created by outside powers only keep going as long as the flow of funding continues. So this will be a long-term commitment.

As those Afghan forces shrink from 352,000 to around 220,000 following the 2014 transition, the question of what happens to demobilized men will require particular attention, so that they do not join militias or the insurgency. Local village police have played a role in filling the vacuum in areas where ISAF and the Afghan forces have a lower profile; but they have also been suspected of abuses and it will be wise to integrate them into the regular police under more stringent command and control as quickly as possible.

The withdrawal of ISAF will be a complex operation. There are 650 ISAF bases and facilities to dispose of (about half will be taken over by the Afghans), over 60,000 vehicles to repatriate and over 150,000 containers to move – and all in a country with no sea ports and only a rudimentary road and rail network.

Overall the Allies have stationed more than $60 billion worth of equipment in Afghanistan. Protecting the transit routes against explosives attacks has required ISAF to pay particular attention to route monitoring and clearance and to improving its counter-IED technologies.

As ISAF will still be around for two more years, all these departures must be coordinated with all the fuel, food and military material that will continue to be brought into Afghanistan. ISAF alone needs 50,000 gallons of fuel a day to sustain its operations. But there is no reason to think this will go badly provided that nations coordinate their repatriation plans with ISAF headquarters.

Most sensitive equipment, such as weapons, ammunition and communication devices will be shipped out by air. The route via Pakistan has finally been reopened and NATO has negotiated transit agreements with Russia and three Central Asian countries (Uzbekistan, Kazakhstan and Kyrgyzstan) for road, rail and overflights. Indeed, Russia has granted NATO the use of a transit hub at Ulyanovsk in Siberia. Although the northern transit route costs the Allies $120 million more a month to operate than the more traditional southern route via the Khyber Pass and Pakistan, those transit agreements with Russia and Central Asian partners have helped to improve overall relations and could prove useful for possible future NATO operations beyond Europe.

There is another major challenge resulting from such a massive logistical redeployment: this is to ensure that all the money that will flow into the hands of local transport or convoy protection companies does not end up with the Taliban or militias as a consequence of protection rackets and extortion.

2014 will not be the end of NATO's engagement in Afghanistan but part of a continuum. After two years of transition will come at least a decade of transformation. Afghanistan will remain one of the poorest countries in the world, and an insurgency of some sorts will no doubt continue for the immediate future. Engaging Pakistan will continue in this respect to be essential, as Pakistan-based insurgent groups, like the Haqqani network, will continue to be responsible for many of the attacks against Afghan and international forces.

Afghanistan will continue to face major problems from corruption, weak institutions and governance, inadequate human rights and women's rights protection and stuttering economic development. Politics and economics will be even more intractable than security. But with a well planned and executed transition, which at least gets the security part of the equation right, NATO can guarantee that ISAF leaves Afghanistan in much better shape than when it found it back in 2003. Afghanistan will continue as a country and as a state with good days and bad days, but with an internal resilience and a desire to move forward that may well surprise us. ■

The views expressed in this article are those of the author and do not necessarily reflect official NATO thinking.

Mali's coat of arms. The motto reads: "One people, one goal, one faith".

Mali's malaise

How to prevent the Sahel from turning into a corridor of conflict | By Alexander Graf Lambsdorff

A vast, rugged terrain, indigenous Islamic fundamentalism, weak governance, and a profound lack of interest in the West – what sounds like a description of pre-2001 Afghanistan is today's reality in large parts of the Sahel. Roughly serving as a demarcation line between the Maghreb and Sub-Saharan Africa, it covers a vast stretch of land from Senegal in the west to Eritrea in the east. But state borders mean little in the Sahel, they are as porous as its soil.

Also, the exact scope of the Sahel is subject to changes that are due to climatic factors such as desertification and drought. As a matter of policy, the Sahel has not been high up on the EU's agenda. Given its proximity to its borders and its relevance in connection with such issues as migration flows, terrorism, and energy security, this needs to change. Fortunately, this change is underway.

Mali exemplifies the regional and transnational malaise. It was caused at least in part by events in Libya and now directly affects Burkina Faso, Algeria, Niger and Mauritania.

For many years, Colonel Qaddafi paid and equipped Tuareg fighters to keep the vast south of the country under control. At the same time, thousands of Malians were given jobs in Libya and supported their families through remittances.

With the downfall of the regime, both groups lost their sponsor. Many of the fighters returned to Mali, well trained for desert warfare, and thousands of black Africans left or fled the country after the revolution – not only did they no longer have jobs, many of them were also suspected of being mercenaries on Qaddafi's payroll.

It is worth noting that Libya and Mali do not share a common border but that traffic between the two countries across the Sahara crosses Niger or Algeria for about one thousand kilometres. Statehood and borders matter little in the ocean of sand that is the Sahara.

In March of this year, a military coup against the Bamako government plunged the country into a phase of dramatic political instability, in the course of which the central government also lost control of the northern Azawad region. There, the returning Tuareg fighters from Libya had joined a fundamentalist Islamic group to take control of all he major cities in the north.

The Islamists immediately began the dramatic curtailment of basic human and civil rights associated with fundamentalist Islam, including stonings and amputations. As a result, about 435,000 Malians have fled their homes, while 250,000 have crossed borders into Burkina Faso, Mauritania, and Niger.

Neither of these countries boasts an impressive level of socio-economic development and they are now faced not only with one state in crisis but with two de facto entities threatening regional stability. Restoring order in Mali will prove difficult and will most likely require a settlement that will leave state authority permanently diminished.

Mali demonstrates that problems in the Sahel transcend traditional Western thinking about the relevance of state borders. The ability to move quickly and freely in large and effectively lawless territories is key to actors like Al Qaeda in the Islamic Maghreb (AQIM), who use the region as a safe haven and power base. They benefit from and aggravate problems in connection with smuggling, trafficking and arms proliferation and fill the power void left behind by struggling governments. Sometimes, local populations even view religious totalitarian rule as the lesser evil, because it at least provides a modicum of stability.

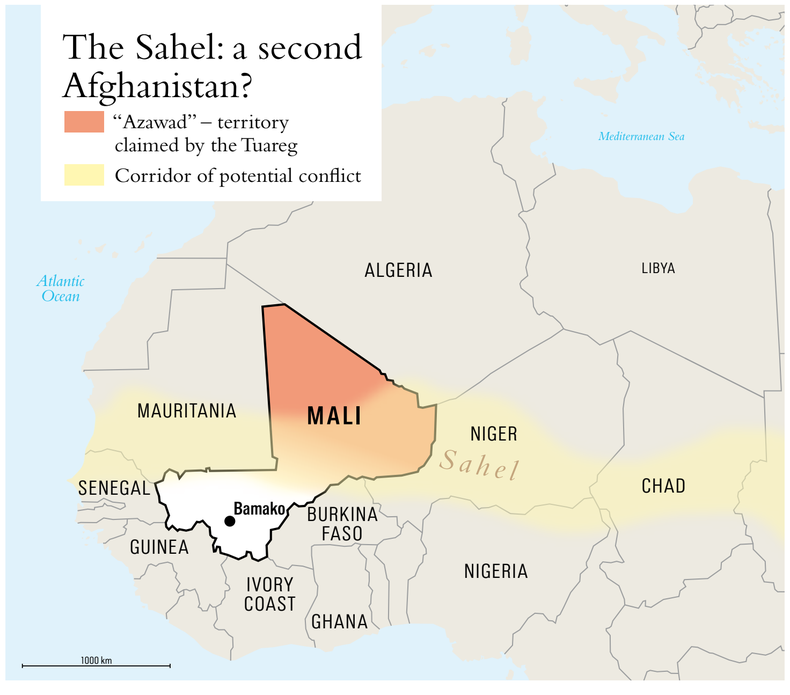
The remedy therefore must equally be of a transnational nature. The EU can use its geographic proximity and experience in regional cooperation, development and capacity-building to foster closer links between the countries largely affected by similar problems.

But it has to link its development efforts with counterterrorism and crime-fighting mechanisms more effectively. Tackling crime and terrorism simultaneously with development and aid efforts has multiple benefits.

Alexander Graf Lambsdorff is a member of the European Parliament's Committee of Foreign Affairs.

SABINE SCHRÜNDER

Flashpoint SAHEL



Apart from the stand-alone virtue of helping to empower the people in the region to build better futures and instil some trust in state institutions, it might help to convince traditionally suspicious ex-colonies that Western involvement is not selfishly geared toward defeating threats to its own citizens, and hence secure a greater degree of cooperation. The menace to their own respective power bases, as exemplified by the Malian case, may help to secure a greater willingness on the part of governments to work together.

In order to achieve tangible results, however, Europe will also have to work with other actors, such as the African Union, Interpol, the UN as well as the United States. A more structured transatlantic approach to the region is in fact a sine qua non for any significant progress to be achieved across the Sahel.

It remains to be seen whether China can be engaged in political cooperation on certain topics. The People's Republic is a preferred interlocutor for many countries of the region and while economic competition with the West will remain, certain strategic interests might overlap, such as anti-terrorism.

Still, the Sahel is facing an uncertain future, and escaping the downward spiral is by no means an easy feat. The more recent crises that have unfolded in the region, like the severe food shortage or the aggressive move of al-Qaeda into the Maghreb have led to a reappraisal of the Sahel's significance among European policymakers. Many of the countries in the area are former colonies of EU member states, which, depending on the nature of today's relations, can be a blessing or a curse.

France, in particular, will have to play a leading role in preventing the Sahel from turning into a second Afghanistan. Accomplishing such a mammoth task, however, will require a collective and coordinated effort by the international community.

The failure to address these issues would have repercussions way beyond the region itself. It might pose a threat to the safety not only of the local populations, but also of European and American citizens. ■

Geopolitics in a cold climate

Fears of international conflict over arctic resources are exaggerated. Clear territorial boundaries make profit-driven co-operation more likely

The geopolitics of the new Arctic entered the mainstream on Aug. 2, 2007. Descending by Mir submersible to a depth of over 4 km, a Russian-led expedition planted a titanium Russian flag beneath the North Pole. The news shocked the world.

The Lomonosov ridge under the pole, which is probably rich in minerals, is claimed by Russia, Canada and Denmark. The Russians, it was assumed, were asserting their claim, perhaps even launching a scramble for Arctic resources. One of their leaders, Artur Chilingarov, Russia's leading polar explorer and a Putin loyalist, fanned the flames. "The Arctic has always been Russian," he declared. Yet the expedition turned out to have been somewhat international, initiated by an Australian entrepreneur and a retired American submarine captain, and paid for by a Swedish pharmaceuticals tycoon.

Even so, fears of Arctic conflict have not gone away. In 2010 NATO's top officer in Europe, James Stavridis, an American admiral, gave warning that "for now, the disputes in the north have been dealt with peacefully, but climate change could alter the equilibrium". Russia's ambassador to NATO, Dmitry Rogozin, has hinted at similar concerns. "NATO", he said, "has sensed where the wind comes from. It comes from the north." The development of the Arctic will involve a rebalancing of large interests. The Lomonosov ridge could contain several billion barrels of oil equivalent, a substantial prize. For Greenland, currently semi-autonomous from Denmark, Arctic development contains an even richer promise: full independence. That would have strategic implications not only for Denmark but also for the United States, which has an airbase in northern Greenland.

There are also a few Arctic quirks that turn the mind to confrontation. Most countries in the region (the United States being the main exception) have powerful frontier myths around their northern parts. This is truest of the biggest: Russia, for which the Arctic has been a source of minerals and pride in the feats of Russian explorers, scientists and engineers since the late 19th century; and Canada, which often harps on Arctic security, perhaps as a means of differentiating itself from the United States.

During the cold war the Arctic bristled with Soviet submarines and American bombers operating from airbases in Iceland and Greenland. The talk of Arctic security risks sometimes betrays a certain nostalgia for that period. Some people also worry about Arctic countries militarising the north. Canada conducted its biggest-ever military exercise in the north, involving 1,200 troops, in the Arctic last year.

Yet the risks of Arctic conflict have been exaggerated. Most of the Arctic is clearly assigned to individual countries. According to a Danish estimate, 95 percent of Arctic mineral resources are within agreed national boundaries. The biggest of the half-dozen remaining territorial disputes is between the United States and Canada, over whether the north-west passage is in international or Canadian waters, hardly a casus belli.

Far from violent, the development of the Arctic is likely to be uncommonly harmonious, for three related reasons. One is the profit motive. The five Arctic littoral countries, Russia, the United States, Canada, Denmark and Norway, would sooner develop the resources they have than argue over those they do not have. A sign of this was an agreement between Russia and Norway last year to fix their maritime border in the Barents Sea, ending a decades-long dispute. The border area is probably rich in oil; both countries are now racing to get exploration started.

Another spur to Arctic co-operation is the high cost of operating in the region. This is behind the Arctic Council's first binding agreement, signed last year, to co-ordinate search-and-rescue efforts. Rival oil companies are also working together, on scientific research and mapping as well as on formal joint ventures.

The third reason for peace is equally important: a strong reluctance among Arctic countries to give outsiders any excuse to intervene in the region's affairs. An illustration is the stated willingness of all concerned to settle their biggest potential dispute, over their maritime frontiers, according to the international Law of the Sea (LOS). Even the United States accepts this, despite its dislike for treaties – though it has still not ratified the United Nations Convention on the Law of the Sea, an anomaly many of its leaders are keen to end.

The LOS entitles countries to an area of seabed beyond the usual 200 nautical miles, with certain provisos, if it can be shown to be an extension of their continental shelf. Whichever of Russia, Canada and Denmark can prove that the Lomonosov ridge is an extension of its continental shelf will therefore have it. It will be up to the countries themselves to decide this: the UN does not rule on disputed territories. The losers will not do too badly, though: given the Arctic's wide continental shelves, the LOS guarantees each a vast amount of resource-rich seabed.

The 2007 furore over the Russian flag led to an important statement of Arctic solidarity, the Ilulissat Declaration, issued by the foreign ministers of the five countries adjoining the Arctic Ocean (to the chagrin of the Arctic Council's other members, Sweden, Iceland and Finland). This expressed their commitment to developing the Arctic peacefully and without outside interference. Possible defence co-operation between Arctic countries points in the same direction. Their defence chiefs met for the first time in Canada in April in what is to become an annual event.

The Arctic Council, founded in 1996, was not designed as a regional decision-making forum, though outsiders often see it that way. Its mission was to promote conservation, research and sustainable development in the Arctic. The fact that six NGOs representing indigenous peoples were admitted to the club as non-voting members was evidence of both this ambition and the countries' rather flaky commitment to it. But since 2007, under Danish, Norwegian and now Swedish chairmanship, the council has become more ambitious. Next year it will open a permanent secretariat, paid for by Norway, in the Norwegian city of Tromso. A second binding pact, on responding to Arctic oil spills, is being negotiated; others have been mooted.

Russia, which has at least half of the Arctic in terms of area, coastline, population and probably mineral wealth, is in the thick of the new chumminess. It has a reputation for thinking more deeply about Arctic strategy – in which Vladimir Putin and his prime minister, Dmitry Medvedev, are both considered well-versed – than any other power, and appears to have concluded that it will benefit more from collaboration than from discord. Indeed its plans for the Northern Sea Route may depend upon international co-operation: Norway and Iceland both have ambitions to provide shipping services in the region.

Russia's ambassador for Arctic affairs, Anton Vasiliev, is one of the council's most fluent proponents of such collaborations. At a recent conference in Singapore, he surprised many by declaring Russia eager to standardize safety procedures for Arctic oil and gas production. "The Arctic is a bit special for civility," he says, "You cannot survive alone in the Arctic: this is perhaps true for countries as well as individuals."

The United States is less prominent in Arctic affairs, reflecting its lesser interest in the region and lukewarm enthusiasm for international decision-making. Although its scientists lead many of the council's working groups on subjects such as atmospheric pollution and biodiversity, it only hesitantly supports the council's burgeoning remit.

Frustrated advocates of a more forthright American policy for the Arctic, mostly from Alaska, lament that the United States hardly sees itself as an Arctic country, a status it owes to its cut-price $7.2 million purchase of Alaska (Russian America as was) in 1867. A common complaint is the United States' meager ice-breaking capability, highlighted last winter when an ice-capable Russian tanker had to be brought in to deliver fuel to the icebound Alaskan town of Nome.

As governments wake up to the changing Arctic, global interest in the region is booming. A veteran Scandinavian diplomat recalls holding a high-level European meeting on the Arctic in the early 1990s to which only her own minister turned up. "Now we're beating countries away," she says. "I've had a couple of African countries tell me they're Arctic players."

Asia's big trading countries, including strong exporters like China and Japan, shipbuilders like South Korea and those with shipping hubs, like Singapore, make a more convincing case for themselves. All have applied to join the council as observers, as have Italy and the EU. Half a dozen European countries with traditions of Arctic exploration, including Britain and Poland, are observers already.

Some council members are reluctant to expand their club. Canada is especially wary of admitting the EU because the Europeans make a fuss about slaughtering seals; Russia has a neurotic fear of China. Even the relaxed Scandinavians are in no hurry to expand the council. Yet the disagreement has been overblown. If the EU, China and others were to be denied entry to the council, they would no doubt try to raise Arctic issues elsewhere, probably at the UN, which is a far more dreadful prospect for Arctic countries. So by the end of Sweden's chairmanship, in May 2013, these national applicants are likely to be admitted.

But Greenpeace, which also wants to be an observer, may not be, even though another green NGO, the World Wildlife Fund (WWF), already is. Several Arctic governments have been put off by Greenpeace's aggressive methods. Greens against governments, not country against country, looks likely to be the most serious sort of Arctic conflict. That is progress of a sort. ■

This article was first published in "The Economist," June 16th, 2012.

The cyber attackers are on the march

Defeating them will require new ways of thinking – and lots of money

By Sandro Gaycken

NEUEBILDANSTALT/RAUPACH

The threat posed by cyber insecurity has intensified. It is now more substantial than ever and the reason is technological progress itself. Complex, multifunctional, networked computers have become the norm in every sector of society. And we have grown dependent on them - we can no longer live or work without them.

Hackers have always been a problem but they never posed a serious systemic threat. They have been on the periphery, an occasional nuisance and sufficiently manageable. Teenage activists disrupted services to attract media attention. Fraudsters abused the anonymity of the web to make money. But the growing dependency on computers for more critical processes has attracted a new breed of hackers: organized crime syndicates and nation states. These new attackers are different. They have more resources at their disposal. They cannot be stopped by our current security concepts. For them, penetrating any kind of technical protection is child's play. Nor do they fear prosecution; they will never be sufficiently identifiable.

FU BERLIN

Sandro Gaycken is a researcher in technology and security at the Free University Berlin, Institute of Computer Science.

These attackers have woken up to the possibilities, stirred either by individual, headline-grabbing events like Stuxnet or simply by the steadily growing stream of bad news related to all sorts of cyber incidents. They are not yet operational. But most experts are convinced that offensive cyber capacities are an important future asset. Once operational, these capacities will be a game changer and IT security will be an entirely different task, one of vital importance. It will also become more difficult, much more complex. The first step in preparing for the change is to anticipate this future. Some developments are easy to predict.

Organized criminals will identify monetarily interesting systems. The preferred target will be the financial industry, which is dependent on a vast landscape of information technology that is just slightly more secure than the norm. The benefits are straightforward. A patient attacker will be particularly successful; A cyber-manipulator of the financial market will not cause crashes or sudden spikes. They will operate multiple tiny events over a stretch of time. That way, no one will ever notice. Neither the technology nor its operators can pay much attention to detail any more, given the complexities of both the financial system and their technical substrate. Undetected attacks can be mounted again and again. In sum: few costs, no risk, tons of money.

Nation states will be interested in power. Militaries and secret services will identify multiple targets and strategies to gain it via cyber-offense. It comes as no surprise that most countries have announced their interest in the topic over the past few years. They will soon have their cyber troops ready – or buy hacks on the open exploit market – and enter into an exploratory phase to test these new tools. They will discover two things.

First, hacking capabilities can support conventional strategies. Classical deterrence can be strengthened in a number of ways. Military hackers will be an elegant and efficient extension of electronic warfare, attacking military technology wherever it runs through a computer. And being able to hack critical infrastructures, banking systems, state institutions, and many other digital veins of information societies will have an additional deterrent effect of it's own. Cyber-warfare will hand a certain advantage to militarily otherwise less potent nations. No matter what their other military capacities are – offensive cyber capacities alone will enable them to credibly threaten high-tech nations. Cyber-warfare might evolve into a global strategic equalizer.

However, the militarily potent nations can and will make use of cyber-deterrence as well. They are likely to start demonstrating their capacities soon. This will carry the potential to initiate escalations: Analysts might be unsure how to interpret them. They might decide to base their response on a worst-case scenario. If they do not know who the attacker was, they might simply choose their favorite enemy – and retaliate. In a climate of heightened tensions and sensitivities towards cyber-incidents, such escalations could spiral into actual conflicts.

The second discovery nations will make relates to the broad spectrum of unconventional strategies enabled by cyber capabilities. One type is particularly likely and worrisome: strategies of silent erosion. These follow the aforementioned paradigm of "running silent" – amassing numerous tiny events rather than delivering single, strong strikes. Attacks would be barely detectable, posing as some kind of business as usual – a minor fluctuation, a single incident causing little harm. But they would be part of a strategy of death by a thousand cybercuts. Their patient, ultimate aim would be to erode the economic or the military might of a nation or even a continent by a continuous stream of low-level incidents. Such a strategy would be cheap, efficient, reliable, and risk-free. And it will mainly target companies. Strategies of silent erosion are best placed in a less secured, yet in sum critical and vulnerable target, where incidents happen on a daily basis anyway – the business sector. In the future, such daily incidents of espionage, sabotage and manipulation might become the geo-strategy of choice for some nations. That in itself might initiate or catalyze escalations. And, states might misinterpret criminal activity as strategic attacks by other nations.

> "Cyber-warfare might evolve into a global strategic equalizer."

The new, resourceful attacker does not represent the usual hubris of progress. It is not a case of one thing coming at the cost of another. Instead, it is a typical, cyclical development of military strategy. A previously successful technological paradigm has critically degenerated into a problem by the development of serious countermeasures. Many such stories are known: The sword became useless against the machine gun; the walled fortress had to be replaced by the bunker with the rise of air power. Only this time, the critically degenerated progress is not just a tank or some military camouflage technology. It spans the whole of society and three quarters of the globe.

This renders the reaction difficult. The usual military response would be to seek to optimize the system under attack, make it resilient and, if that is not possible, to scrap it and adopt a different approach. But can we abandon complete IT systems and start over? In part, yes: We don't really need all the computers and networks we have now; quite a few systems can and should be disconnected and downgraded back to 1980s standards. But many segments of society cannot abandon the computer. So, can we optimize security to a sufficient degree? Not within the current IT framework. Maintaining an inherently insecure IT infrastructure and bolting some more or less reliable security products on top has not provided anything like the required level of security in the past and it will not do so in the future. A reform of IT technology is required.

But that is an expensive and complicated undertaking. Any new system first has to be designed and then the whole existing environment has to be replaced. We need good reasons to undertake such an effort. We do not really have them, not yet. What we do have is plenty of scaremongering from stakeholders with a vested interest in creating a climate of fear, and some scientists – like this author – sketching somewhat hypothetical future scenarios. The more prosaic reality, as far as the general public is aware, encompasses blocked websites, stolen customer data, and credit card fraud – none of which represents a major systemic threat. So should we wait for the future to happen and then react? That could be too late. And in fact serious cyber incidents are already occurring to a sufficient degree to initiate reform. We know they are out there but they are not being disclosed: Companies fear for their reputation and their stock price; States fear admitting to tactical disadvantages.

This secrecy shrouding cyber incidents is a major problem. It creates what is probably the biggest threat at present: uncertainty. No one knows what is happening, if anything is happening at all, what it means if something is happening, and what could really improve the situation. That gives rise to an uncertain threat perception in general and a good deal of insecurity among decision-makers in particular, leading to some counterproductive reactions.

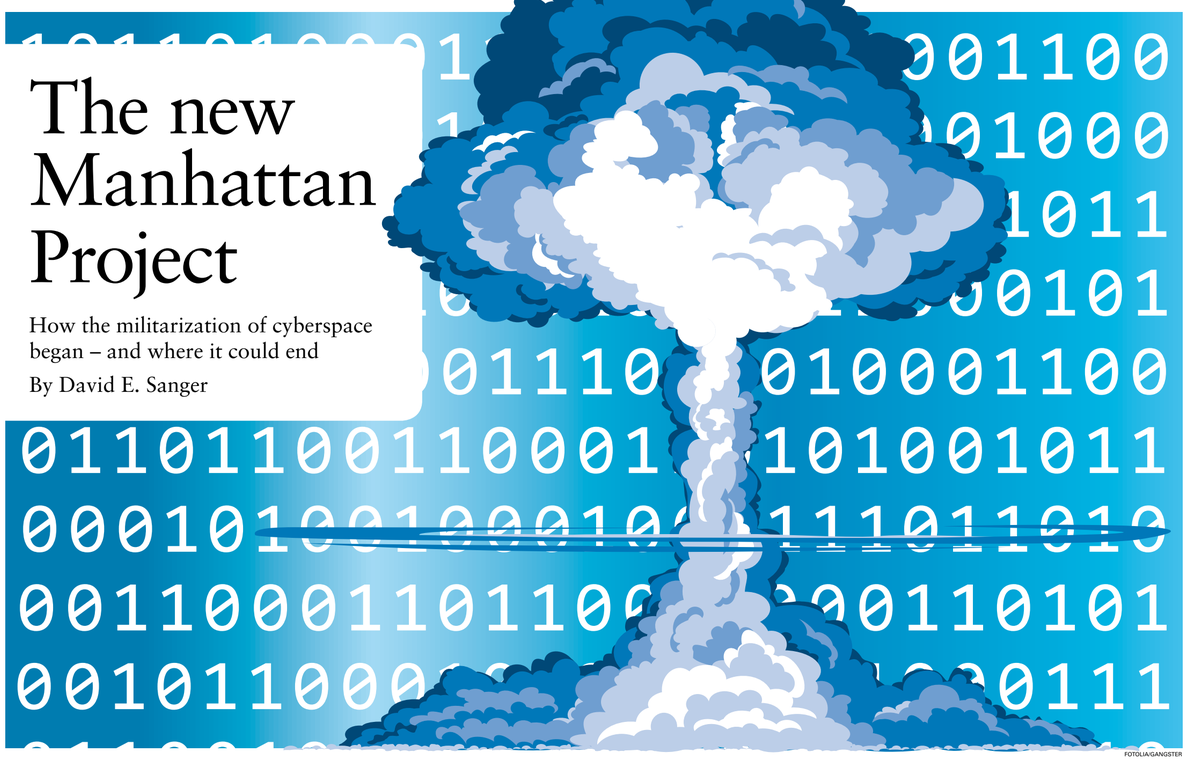
No one wants to speak openly about it, because anything they say could turn out to be wrong. So there is no debate. No one wants to risk an unconventional approach in case they end up taking the wrong decision. So conventional, conservative, non-reformatory reactions are favored – even if they have failed to provide security in the past decades. And no one wants to waste money combating vague risks. So countermeasures have to be cheap. Paradoxically, all this might cause a costly delay. Getting IT security right, against the background of these insecurities and hurdles will take many more years – a time span that some actors will interpret as an open window of opportunity, probably at significant cost to their victims.

It is crucial, therefore, to initiate a genuine shift toward an age of effective IT security as soon as possible. Disclosure will be an important first step. Both the state and the private sector must enable themselves to detect incidents, and should publicize the details: the actual or potential damage, the depth and the duration of attacks. This will require courage – the courage of decision-makers. Only if we are as open as the immediate security of the systems permits – and there is still a lot of room for that – will we be able to foster an informed and appropriate evolution of information security, and the necessary reform of information technology. ■

The new Manhattan Project

How the militarization of cyberspace began – and where it could end

By David E. Sanger



FOTOLIA/GANGSTER

Just days before Barack Obama was inaugurated as the 44th president of the United States in January 2009, he arrived at the White House for one of the most important, least-publicized rituals in the transfer of power in America: the private conversation between the departing commander in chief and the incoming one.

This one promised to be tense. The two men had almost nothing in common. They viewed the world entirely differently: Obama had been elected arguing that Bush had alienated allies, failed to talk with adversaries, and plunged the nation into ill-conceived, expensive conflicts that bred resentment of America around the world.

But that day, Mr. Bush told his successor that no matter how severely Obama denounced Bush-era excesses on the campaign trail, the new president would soon come to appreciate two secret programs that Bush initiated. The first was barely secret at all: the American drone program over Pakistan, which Bush had begun to use as his chief weapon for reaching into tribal lands to eliminate al Qaeda's leadership. The second was, in fact, among the most closely-guarded programs in the American intelligence world: A program called "Olympic Games" that Mr. Bush had approved in his last two years in office, as Iran sped forward with its uranium enrichment program.

PRIVATE

David E. Sanger is 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." (Crown, 2012).

Bush proved to be right: Within a year, the new president had doubled down, then tripled down, on both programs. When the history of cyber-warfare is written, "Olympic Games" will undoubtedly be recalled as the beginning of a new age, one in which cyber-weapons became a critical, if still unacknowledged, element of the American arsenal. It is only a bit of overstatement to say that Olympic Games became the Manhattan Project of cyber, the program in which a new weapon's possibilities, and its limitations, became evident to the world. And while the analogies between the nuclear era and the emerging cyber era can easily be taken too far, there are some legitimate comparisons worthy of thought – and a few provide cautionary tales.

The motivation behind Olympic Games was two-fold: to slow Iran's progress, and to give Israel an alternative to a military attack.

Both were urgent priorities. It was evident to Obama by the end of his first year in office that his talk of "diplomatic engagement" with Iran was not yielding much. Efforts to talk directly to the Iranian people had accomplished little; private letters to the Supreme Leader, Ayatollah Ali Khamenei, drew responses that could best be described as diatribes about decades of American misjudgments and malfeasance in the region. Obama had quietly accelerated the groundwork for far more extensive economic sanctions against Iran, but they are slow to develop and require extensive cooperation from Iran's major trading partners, which seemed unlikely at the time. So the idea that the US could deploy, with Israel, cyber-weapons that stood a chance of crippling an adversary's nuclear infrastructure, without dropping a single bomb, seemed enormously appealing. In short, the United States could accomplish with computer code what previously would have required an air attack or sabotage on the ground.

Best of all, in Obama's mind, the attack would be hard to attribute to Washington or Tel Aviv. The intelligence gleaned by the National Security Agency and Israel's Unit 8200, which cooperated on planning and implementing the attacks, indicated that the Iranians were mystified by what was happening to the centrifuges at Natanz. The engineers at the plant had assumed, naively, that walling their computer systems off from the Internet would protect them from viruses, worms, and other attacks. (Many American and European companies have similarly proven overconfident in the ability of an "air gap," essentially an electronic moat, to protect their most sensitive systems.) When the centrifuges began speeding up or slowing down, destabilizing the giant machines until they exploded, many experts assumed it was a manufacturing error. After all, the Pakistanis had sold Iran an old, outdated, and unreliable design, the so-called "P-1" centrifuge that Pakistan itself had abandoned. That was exactly what the designers of "Olympic Games" had counted on; as long as the Iranians could not tell an accident from sabotage, they could not solve the problem.

Over the next two years, Obama would descend into the Situation Room regularly for a look at "the horse blanket," a huge fold-out map of the Natanz plant. Officials from the intelligence world and the Pentagon would brief him about the progress of the latest attacks, and discuss their future plans. Vulnerabilities in the Iranian design were identified. Almost every time, Obama authorized requests that the program accelerate, with bolder and bolder attacks. New versions of the worm were inserted every few weeks or months, slipped in on memory sticks or other devices, targeting specific groups of centrifuges.

It all worked spectacularly – until one day in the early summer of 2010, when a programmer made a mistake. (There is still a running argument over whether it was made by the Americans, the Israelis, or both.) The worm that was intended to stay inside the Natanz plant managed to escape, aboard the laptop computer of an unwitting engineer. When he connected to the Internet, the worm replicated itself – without realizing its environment had changed. Soon the worm, quickly dubbed "Stuxnet," was showing up everywhere – in Iran and India, then in Indonesia and soon around the globe. Computer professionals began picking apart the code. Quickly, they found the silver bullets aimed at the heart of Iran's enrichment program.

> "Has the United States legitimized the use of a new weapon of war, one that could easily be turned on America or its allies?"

At that moment, the cover was blown on the program. The Iranians knew they were under attack, and they didn't think the Swiss were behind it. They accused the US and Israel. But they were not certain what to do about it, or how to protect themselves.

Inside the White House, a major decision loomed. Should Obama kill "Olympic Games," or keep it going? It was the subject of considerable debate in a Situation Room meeting with Obama, Vice President Joe Biden, and the director of the CIA at the time, Leon Panetta. Eventually, Obama concluded that it would take a while for the Iranians to figure out the attack, and to design a way to counter it. In the meantime, the next versions of the worm could be unleashed. It was a good call. Soon the worm had its biggest success: It took out nearly 1,000 centrifuges. Iran removed far more machines, for fear they, too, would be destroyed. The first sustained cyber attack by one nation on another appeared to be a success.

But we now know that the success was relatively short-lived. Now aware that they were under attack, the Iranians designed preventative action. In the end, according to estimates inside and outside the US government, Stuxnet bought maybe a year, maybe 18 months, of delay. Yet now, two years later, the data shows that the Iranians have installed nearly three-quarters of all the centrifuges they can put inside the deep underground site at Qom – one largely invulnerable to Israeli attack – and their production of enriched uranium has resumed.

Now Washington, and the world, has to deal with the aftermath. Suddenly many are asking the question that Obama himself asked during the debates over Olympic Games: Has the United States legitimized the use of a new weapon of war, one that could easily be turned on America or its allies?

By all accounts that was only one of the issues nagging at the President as he ushered the United States into a new age of cyber-war.

As a candidate in 2008, when Obama spoke about cyber threats it was mostly in terms of protecting the United States and assuring the privacy of American citizens, whose medical and credit card data was at risk of exposure.

But the militarization of cyberspace raised a host of new issues. First among them was the question of when the United States should use a cyber weapon. The decision to attack Iran was straightforward: In Obama's mind, it was a way to avoid war, not to start one. But what of other, more complicated cases?

So far, Washington will not engage in that subject in public. It cannot, since it does not acknowledge possessing or deploying cyber-weapons. But sooner or later the country is going to have to debate when to use cyber attacks. And that is not likely to be a short debate.

Just think: It took years after the United States dropped the atomic bomb on Hiroshima for the nation to develop a common national understanding of when and how to use a weapon of such magnitude. Not until after the Cuban Missile Crisis, 50 years ago, did a consensus emerge that the weapon was too terrible ever to employ again, save as a deterrent and a weapon of last resort.

Today we are going through a parallel debate about how to use Predator drones. President Obama has taken to the Predator for the same reason he has embraced cyber-attacks: the Predator is a precision instrument. Civilian casualties are reduced. Properly targeted, he believes, cyber weapons are far less likely to harm innocent civilians. In short, the lawyer inside Obama is willing to put constraints on the military commander inside Obama.

But it is far from clear that other countries, or terror groups, would have similar rules, or Obama's compunctions about attacking civilian sites, or hospitals, or even financial systems.

And to deter such attacks, the US has to make it clear that it is willing to counter-attack. But there is nothing so simple about responding to cyber-attacks. Usually it is unclear where they come from. That makes deterrence extraordinarily difficult. Moreover, a good deterrence "has to be credible," said Joseph S. Nye, the Harvard strategist who has written extensively on the lessons of the atomic age, and tried to apply them to cyber war. "If an attack from China gets inside the American government's computer systems, we're not likely to turn off the lights in Beijing." But the temptation to respond in some non-lethal way will be overwhelming.

As the American infrastructure for fighting cyberwar grows larger, these questions will grow more urgent. Already there is a United States Cyber Command, located at the National Security Agency headquarters midway between Washington and Baltimore. The Air Force has a new cyber wing, with thousands coming to work each day thinking about new strategies for offense and defense. And there will undoubtedly be successors to "Olympic Games," because all the other options for slowing Iran are either long shots, or two difficult to contemplate. In short, this is a weapon for a new age, but as a society, we have yet to decide how, or if, we can control it. ■

The world needs a new cyber watchdog

International cooperation is the only way to deter online warfare

By Eugene Kaspersky

FOTOLIA/JEFF GYNANE

Cyber-warfare" as a term is slowly but surely permeating into public consciousness around the world. First came Stuxnet, followed by Duqu, then Flame, and just recently we discovered Gauss – all sophisticated malware cyber-weapons used for cyber-espionage or cyber-sabotage – or both. They represent the relatively new trend of cyber-warfare, attacks carried out by nation states on other nation states using computer software as a weapon.

Cyber-war attacks can sabotage vital modern-day life-supporting infrastructure.

PRIVATE

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

Destroy it, and the consequences would be catastrophic. Think reservoirs, air traffic control, and the food chain. All modern infrastructure is highly computerized and networked and globalization means that a lot of infrastructural technology, such as SCADA (Supervisory Control and Data Systems), is identical the world over. It can all become vulnerable to state-of-the-art cyber-attacks, even to the extent of the attacker country becoming a victim of its own cyber-weapon – the so-called boomerang effect.

As regards attribution, pinpointing precisely who is behind a given cyber-attack continues to be practically impossible due to cyber-weapons' anonymity. One can never tell for sure where a cyber-weapon was developed, or to whose order, as any such hard data – proof – simply never exists in a cyber-weapon. Attribution can only be guessed at, for example, by programmers' comments that are sometimes left in the code, or the political context of an attack (who would benefit?).

However, what we do know is that increasing use of cyber-weapons is linked to acts of state-backed cyber-war, and not merely (non state-backed) cyber-crime or cyber-terrorism. This can be fairly reliably assumed when one looks at the cyber-weapons' sophistication, and also the respective budgets – millions of dollars – that must have gone into achieving that sophistication.

This is what is most frightening about cyber-warfare: it is extremely well financed, and therefore the results it can achieve can be the most far reaching and damaging – even paradigm shifting.

The continuing uncovering of cutting-edge cyber-weapons also indicates how secret services and/or militaries are becoming increasingly active in cyber-armament and deployment in addition to their more traditional roles. As a result, the Internet – the key enabler for most cyber-weapons – is becoming increasingly militarized. None of this can be deemed a good thing – either for humankind or the planet it inhabits.

With cyber-warfare on the rise, governments should, at least in theory, be open to taking steps to responsibly agreeing to certain controls on cyber-weapons in the interests of their electorates and of course of national and world peace. If nation state-backed development of cyber-weapons continues unabated, the day may come when, heaven forbid, terrorists get a hold of them.

In fact, this scenario is likely. All it takes is one slip-up to cause details of a "secret" cyber-weapon to be released out into the wild. Once there, it is fairly easy for the technology to be stolen, copied and adapted, and before you know it a "new" cyber-weapon has wound up in the hands of goodness knows whom.

So, faced today with the ominous prospects of cyber-warfare's disastrous consequences, what realistic potential is there for some kind of control of the escalating situation?

I believe the only way to deter cyber-warfare in general is in international cooperation. I think an "International Cyber-Security Organization (ICSO)" should be created, which would act as an independent platform for global cooperation, leading hopefully to treaties controlling cyber-weapons in the same way the International Atomic Energy Agency (IAEA) controls nuclear weapons and other international treaties control chemical or biological weapons. Such an ICSO would also be best placed to investigate cyber-attack incidents by uniting the entire world's leading IT Security research community.

> "If nation state-backed development of cyber-weapons continues unabated, the day may come when terrorists get hold of them."

Of course, we need to be realistic; the ICSO would not be able to eliminate cyber-weapons completely. But it would at least greatly improve the situation as it stands at present. It would be a good start.

But a world cyber-authority is as yet still a pipe dream. It is all very well in theory, but the hard bit comes in getting all the key nation states to the negotiating table. Harder still is getting all states to agree to some kind of rules of the game – as some states might not want to abandon, or even admit to, their hard-won (in terms of education and investment) secret know-how advantages that they might be planning to use or are making use of currently.

It looks likely that it will be highly developed industrialized nations that will eventually take the lead in an international cooperation initiative. One principal reason for this, besides their traditionally leading the way on such joint projects, is that they are the countries that are most vulnerable to cyber-war attacks as they have the highest Internet (cyberwar-enabler, or weak-link) penetration.

In the meantime, what can countries do to protect themselves?

First of all it needs to be understood that it is almost impossible for countries to fully protect themselves from cyber-war attacks today. To do so it would be necessary to practically rewrite just about all the software code in existence for secure operating systems. This is simply unrealistic – far too expensive.

Protection is more difficult the more a country has lots of essential services online. Many of these services are managed by different local authorities inside a country. This means they may have different security tools, sometimes different policies, and so on.

So the first step would be to have a national security defense policy, which must be adhered to at all critical points. The second step would be developing a risk management approach and extending cyber-security to critical infrastructure. Monitoring is another very important task: it needs to be sufficiently flexible while extremely intelligent. And let us not forget about improving cyber-education of the population.

On a smaller scale, I am often asked if average home users or companies should be at all worried for themselves personally with news of the ongoing growth in cyber-warfare. At first, the answer might be expected to be no. Stuxnet, etc. were designed as highly targeted cyber-weapons aimed mostly at the Middle East. Why would someone in, say, Iceland, be at all worried?

Well, besides the accidental side-effects mentioned above that could affect critical infrastructure elsewhere – including in Iceland – once malware is in the wild it can travel to practically any point in the world via the Internet (via, for example, a socially-engineered e-mail attachment or drive-by download). Or, if USB sticks are used for propagation, what's not to say your neighbor in Iceland was given an infected USB while on a business trip in Lebanon, from which he showed you his photos of the trip after the barbeque Saturday night?

Unlikely? Sure. But that Lebanon-to-Iceland scenario has to occur just once – anywhere – for the malware to be spread where it wasn't intended, and from there it could spread exponentially all over the globe, affecting anyone, maybe everyone, including the attackers' country. And by everyone I mean literally everyone – individual users, companies, governments, and whole countries – since it will be homogenous infrastructure, operating systems and software running on the systems we use in everyday life that will come under attack. ■

FOTOLIA/VLADISLAV KOCHELAEVS

It's the economy, stupid!

Cyberwar is a new kind of threat, targetting infrastructure but also business, through piracy

By Toomas Hendrik Ilves

In the past 20 years, Estonia has pioneered the use of Information and Communication Technology in government. ICT was the best, if not only way to leapfrog decades of backwardness resulting from Soviet occupation. Information technology and its use in the public as well as the private sector was the engine of our rapid development, enabling us to become a leader offering innovative solutions, which we gladly share with others.

Almost as if on cue, we also became the world's first victim of deliberate, directed, massive and across-the-board cyber-attacks – and, therefore, one of the world's centers of cyber-defense and security.

Five years ago, in April-May 2007, Estonian government sites, banks, newspapers, even the emergency number 112, were hit by so-called distributed denial of service attacks (DDOS), overloading servers. These attacks were politically motivated, yet they utilized criminal networks – botnets, the hijacked PCs of innocent users who had inadvertently downloaded malware.

Toomas Hendrik Ilves is the President of the Republic of Estonia.

PRIVATE

The main use of botnets is spamming. Controlling malware-infected computers is illegal everywhere, so botnets are run mostly by organized crime.

The cyber attacks against Estonia were not technologically unique – DDOS attacks had been used for years in economic crime – but it was a first in that it was political, a coordinated response to the Estonian government decision to move a statue of a Soviet "liberator" to a less disruptive place. Taking down government and private sector websites in a country highly reliant on Internet services was the continuation of policy by other means, which, as we know, is how von Clausewitz defined war. In a word, the cyber-attacks were a first in that they were directed at a country and they were ordered by someone, i.e. organized; they were political and thus ultimately, an act of war. Few if any wanted to admit this at the time.

Moore's Law, the empirical observation that the computing power of a chip doubles every 18 months, has a corollary in cyber-conflict. Today's cyber-attacks are far more sophisticated than the decade-old use of DDOS attacks. Stuxnet-type worms can disrupt and destroy the ubiquitous Inter- and Intranet based control systems that run everything from our critical infrastructure to our cars and refrigerators. Industrial Control Systems (ICS) have made modern life far more comfortable and efficient, yet at the same time made us even more vulnerable.

Yet, I believe we concentrate far too much on the so-called hard security side of cyber. The real battles are ongoing and affect our security and well-being in altogether different ways than is generally discussed. Perhaps we are too fixated on militarization of cyber rather than state-sponsored theft. Slowly, the understanding is dawning that warfare need not always hit state or civilian infrastructure, but can also target our business sector, through piracy. In other words, in the immortal words of Bill Clinton: "It's the Economy, Stupid."

Espionage against states and increasingly against the private sector, especially areas dependent on R&D and intellectual property, is the other growth industry in an era of exponential computing growth. State and non-state actors including hackers and organized crime groups often work in a unique form of private-public partnerships to steal intellectual property that represents a company's hundreds of millions of euros and years-long research and development.

Let's face it: our companies are coming under massive attack. This is true everywhere in the West, where intellectual property is a key component of our national wealth. It may be difficult to steal a country's oil or its agricultural or even manufacturing wealth, but given the billions, as well as years invested in intellectual property, it can be all stolen in a matter of minutes or a weekend. This is industrial-strength piracy and a genuine security threat, not just a worry of Hollywood film companies.

For technologically advanced countries, including my own, with Tallinn as the R&D center of our flagship company Skype, it is the theft of intellectual property that can in fact cripple or at least severely wound our economies. Let's be sure about this: much of what makes modern economies function and prosper is the product of huge R&D investments, both public and private.

The EU has set a goal for its member states to invest 3 percent of GDP in R&D, a goal few meet (but then again few meet the NATO goal of defense expenditure of 2 percent of GDP). Much of the democratic West's primacy rests on innovation, on new designs, pharmaceutical products, software solutions etc.

A company that invests hundreds of millions or even billions of dollars or euros in new products can see it all evaporate if the research is stolen: the value of the product comes from those years of creative work and money invested in developing it. Yet it can all be stolen. At which point someone else somewhere else has gotten for free what your country's best and brightest spent years to develop. You lose the tax revenue, someone else reaps the profits.

This is piracy. Pure and simple. And it is as dangerous and threatening for modern states as piracy in its more primitive forms off the Barbary Coast was at the beginning of the 19th Century or in fact today off the coast of Somalia. As is the case with classical marine piracy, intellectual property piracy is not only a threat to our economies, it is also a threat that falls into the category of PPP or public-private partnership, where state actors condone or turn a blind eye to it, if it benefits their economies, or even explicitly make use it as the Barbary States did under Ottoman rule. And as with the Barbary pirates, cyber-attacks against our companies can be met head on only with cooperative and concerted state action.

Proceeding from this, the major concerns we have to deal with include: paralysis or destruction of critical infrastructure that today is largely computer-run; espionage, against both governments and the private sector; lack of public trust in electronic databases; lack of all-inclusive databases. This in turn means we must take a multi-track approach: defense of critical infrastructure is a task for governments and NATO, defense of the private sector requires a rethink of government and private sector relations.

In Spring 2008, NATO established its Cooperative Cyber Defense Center of Excellence in Tallinn, serving as a valuable source of expertise in the field of cyber-defense for both its sponsoring nations and NATO. Its interdisciplinary approach to cyber-defense is what makes the Center unique: experts from different fields work together and share their knowledge, giving the Center and its work a broader perspective. The Center aims to become the main source of expertise in cyber-defense by accumulating, creating, and disseminating knowledge in related matters within NATO, NATO nations and partners.

At the end of this year, the Center will publish a National Cyber Security Framework Manual meant to support allies and partners as guidance to develop, improve or confirm their national policies, laws and regulations, decision-making processes and other aspects of national cyber-defense. The target audience will be all stakeholders of national cyber-defense including leaders, legislators, regulators and service providers.

In addition, the Center also offers opportunities to train specialists to deal with potential cyber-attack through the Live Fire Cyber Defense Exercises, such as the annual Locked Shields exercise. The goal is to involve as many participants as possible so that specialists of different countries can practice in real terms what it feels like to cooperate at times of crisis.

The Center also aims to give more support to NATO exercises, such as the annual Cyber Coalition and to the 2012 NATO Crisis Management Exercise. Ideally, cyber should become an integrated component to every NATO exercise.

We will have to rethink government-private sector relations. While Freedom House ranks Estonia as number one in the world in Internet freedom (followed by the United States and Germany), we need to ensure that the freedom is secure from those who would abuse it. Yet if the basis of our relative economic success, our private sector, is coming under attack from state actors, we need to come up with new ways of talking to, and sharing with, the private sector. This of course runs against the grain of how we have often been doing things. Yet we need to address the problem. As I see it, there are two issues.

Firstly, we need to come up with new ways to talk to the private sector. Security clearances, sharing of sensitive information – in both directions from government to private sector and vice versa needs to be made far less ad hoc, far more based on rules that would allow us a greater deal of flexibility to face new threats without at the same time allowing the crony capitalism that destroys democracies.

Secondly, however, we on the state-side of things need the brains that go to the private side of ICT. Let's be honest, Estonia can't pay for the genius software developer at Skype. But then again, the US Department of Defense most likely is not able to hire the top guns at Apple, Microsoft or Google either. The other side(s) can. Back during the Manhattan Project, the US could hire Edward Teller or Robert Oppenheimer for a professor's salary. But nuclear physicists could only work for a university or for the government. Today neither the university nor the government can afford the modern cyber equivalents of an Edward Teller.

All this puts governments at a disadvantage in developing cyber defense. We cannot necessarily afford the best and the brightest. Here in Estonia, however, we have developed one solution to this problem, the Cyber-Defense League, which we can translate, depending on your own national version as the Cyber Home Guard or the Cyber National Guard. These are weekend warriors with ponytails, computer geeks who have high-paying day jobs running IT departments, working in software companies, banks etc., who find it cool to volunteer for their country. We offer them the opportunity to help with our defense. Not running around the woods in camouflage suits but building our cyber-defense capability. They are motivated and patriotic, and let's be honest, it's sexy to work on these things.

> "… during the Manhattan Project, the US could hire Edward Teller and Robert Oppenheimer for a professor's salary … Today governments cannot afford their modern cyber equivalents."

I mention this initiative as the kind of creative solution that we need to begin to consider to be able to guarantee the highly sophisticated e-services and the high R&D driven companies a modern society depends upon. When threats are no longer classic threats, our responses can no longer be classic either – at least if we want to maintain the upper hand.

This means that we need to give new impetus to the otherwise shop-worn concept of co-operation. Governments and states need to get out of the intelligence paradigm where nothing is shared with allies, to a paradigm of interoperability and common response. The private sector and the state need to negotiate new forms of co-operation that will initially be uncomfortable for both but which are the sine qua non of maintaining our economic well-being.

Estonia's experience in the past 20 years reflects this: we are e-believers. We are proud of being pioneers in e-government. And we are convinced that a public sector ICT approach that is citizen-centered, secure and transparent is the future of good governance in the 21st century. ■

Securing the Republic – online

The Federal government has set itself the goal of achieving effective cyber-security cooperation in Europe and the world

By Hans-Peter Friedrich

Within just a few years, rapid technological progress in the cyber field has brought opportunities for networking and innovation which not long ago we could not even have dreamed of. And this progress continues at high speed, so that we have no idea what new possibilities tomorrow will bring.

Today, 40 percent of global added value is based on information and communications technology. Thanks to digital technology, people are connected across national borders and continents, and value chains stretch all around the globe. Whether we are conscious of it or not, IT has become an integral part of our daily lives.

From smartphones, electronic cash and car park guidance systems to the energy and water supply, everything about our daily lives runs on IT. Government, society, business and industry thus depend on cyberspace that functions reliably. The more networked we are, the more dependent we are: This technological quantum leap has created new vulnerabilities we must respond to.

Government, society, business and industry face the common challenge of taking advantage of the opportunities offered by information and communications technology while keeping the risks associated with this interconnectedness as low as possible. All those involved must deal with these opportunities and risks appropriately and rationally.

In addition to greater awareness of cyber-security, we must – nationally and internationally – develop a security culture, which will enable us all to profit from this progress. We must take suitable precautions to make sure that all segments of society can use cyberspace and to keep the risks inherent in such global interconnectedness to an acceptable minimum.

At the latest since Stuxnet in 2010, we know that even processes and systems not directly connected to the Internet are vulnerable to attack. The potential damages from IT failure are enormous. Spectacular incidents such as Stuxnet, Duqu, Flame and the like are only the tip of the iceberg. We are seeing widespread abuse of cyberspace as a place to assert political, military and economic interests.

While the number of attacks remains high, attackers are increasingly focused and professional, and a sophisticated criminal shadow economy has developed on the Internet. Attackers can simply shop for the services they need – they can even buy the complete package to carry out attacks, including support, bulk discounts and guarantees.

Unfortunately, most of these attacks are successful, because too many people still pay too little attention to basic security precautions. We must expand and intensify our efforts to inform and advise, as we are doing at the national level with the botnets information campaign run jointly with the industry association eco, for example, and with our National Cyber Response Centre.

Cyber security must focus in particular on core infrastructure areas on which our government and society are especially dependent. For example, in Germany we have been working closely with operators of critical infrastructure since 2005 within the framework of our CIP Implementation Plan. In that plan, the single points of contact, which are sector-specific reporting centers and links between companies, sector and the Federal Office for Information Security, have proved especially useful. They connect government and the private sector and allow information on IT security incidents to be shared and consolidated. This cooperative approach must be further strengthened and expanded.

Cyber security can and must be guaranteed primarily through preventive measures. Here, government has a dual role: As one actor among many, it must ensure the cyber security for its own area. But it must also create the necessary framework for the IT security measures of stakeholders, on which the security and prosperity of the entire country depend. For this reason, the Federal Government's Cyber Security Strategy adopted in February 2011 pursues a comprehensive approach, which includes all types of IT incidents and is based on shared responsibility by all stakeholders. Thus cyber-security is firmly anchored in the overall system of national security.

The Cyber Security Strategy places a priority on prevention and response, which includes measures to protect the federal information systems and critical infrastructure as well as counter-intelligence and law enforcement measures to fight criminal cyber-attacks.

A key element of the strategy is intensifying information-sharing and coordination between stakeholders. To do so, we have created the National Cyber Security Council, which is made up of state secretaries at the federal level and representatives of the German states and coordinates cyber-security measures at the strategic policy level.

The private sector is also represented by means of associate members. We created the National Cyber Response Centre to be a platform for cooperation among the security authorities (Federal Office for the Protection of the Constitution, Federal Office of Civil Protection and Disaster Assistance, Federal Criminal Police Office, Federal Intelligence Service, Bundeswehr, Federal Police and Customs Criminological Office) and the Federal Office for Information Security. At the National Cyber Response Center, the participating agencies can share information on IT incidents, tools and patterns of attack, attacker profiles and impact of attacks and can rapidly produce consolidated situation reports as needed.

Hans-Peter Friedrich is the German Federal Minister of the Interior.

BMI

The Cyber Alliance founded by the Federal Office for Information Security and BITKOM 2012 will be able to assist a broader range of stakeholders in the private sector and public administration in carrying out appropriate cyber-security measures. It also helps ensure effective, long-term protection of IT through sharing information and experience.

Because even private networks not directly connected to the Internet, such as those used in critical infrastructure, are vulnerable to attack, government also needs to assess the need for action to avert serious cyber-attacks, which could threaten lives, health or society's ability to function. For example, how can the necessary powers be consolidated at the national level following the model of other countries like the US? How can we prevent serious attacks in case of imminent threat even beyond our borders? We will have to ask ourselves these questions if we want to be prepared for the risks that come with cyberspace in the future.

We need to find shared solutions at the level of the international community as well. Almost all industrialized countries are considering how to deal with the growing threat of cyber-attacks. In its Cyber Security Strategy, the Federal Government has set itself the goal of achieving effective cyber-security cooperation in Europe and the world. At the international level, we are working to draw up a code of conduct on security and confidence-building measures in cyberspace. In the process, we are discussing the prevention of cyber attacks and governments' responsibility for actions launched from their territory.

The Federal Government's Cyber Security Strategy ensures that Germany is well prepared to face the international challenges of cyber-security. We must implement, update and expand this strategy step by step. If we all work together, we will be able to take advantage of the enormous potential offered by cyberspace and its rapid development without interference from the related risks. ■

@War

The development of cyberspace as a military domain

By Michael Hayden

I first encountered "cyber" as a military issue when I arrived in San Antonio, Texas in January of 1996 to take command of the Air Intelligence Agency. In my previous posting as Chief of Intelligence for US Forces in Europe I had spent most of my waking moments attempting to deal with the Balkans and the lingering after effects of the battle of Kosovo Polye of 1389. On arrival in Texas, I found that I had gone from the most medieval to the most modern of challenges.

Luckily, I had a good staff in Texas and US Air Force thinking about cyber was quite advanced. My staff began to educate me on the concept of cyber as a "domain" – a place where the American military would ensure American freedom of action while also holding in reserve the ability to deny such freedom of action to others.

Land, sea, air, space....cyber. To an American military officer the concept of cyber as a domain is curiously liberating. If it were a domain it would have, like the other domains, its own peculiar characteristics: this one was inherently global, inherently strategic, characterized by great speed, characterized by great mobility. We knew how to deal with that, no matter how complex the technology.

And if cyberspace were a domain, habits of American military thought would drive one to the conclusion that combat here could be decisive, the same way that the sea domain was decisive at Trafalgar, the land at Gettysburg, and the air in the battle of Britain.

If decisive effects could be achieved in the cyber domain, then there had to be circumstances where action in the other domains would be merely supportive, the way naval bombardment could support a land invasion (Normandy) or ground forces could be used to seize needed airfields (Iwo Jima).

And if American military doctrine was developing along these lines, it was only a matter of time before military organization would follow and a command dedicated to the new domain would be formed.

US CYBERCOM – charged with the "conduct of full spectrum military cyberspace operations" – was formally established in June 2009, the product of the almost relentless doctrinal logic described above. Indeed, CYBERCOM had been anticipated by several predecessor organizations on which it was eventually built. In 1998 a joint Department of Defense and Intelligence Community Information Operations Technology Center was formed at NSA that expanded DoD and IC thinking and developed new concepts and technologies for integrated Computer Network Operations. Later a joint task force (also at NSA) under the unwieldy name of Joint Functional Component Command-Net Warfare expanded both offensive thinking and tools.

As CYBERCOM was organizing itself, the most seminal American policy piece to date on cyber appeared in the September 2010 issue of *Foreign Affairs*. It explicitly labeled cyber as a domain, emphasized its inherent dangers, laid out the doctrine of active defense and outlined the role of the new command as "part sensor, part sentry, part sharpshooter."

But the most important line in the piece may have been the one under the title: "By William J. Lynn III, Deputy Secretary of Defense." Not the Deputy Attorney General. Not the Deputy Secretary of Commerce. Not the Deputy Secretary of State.

> "Does a file on a server in say Houston or Bonn enjoy the same kind of sovereignty that the building or the neighborhood in which it is located does?"

Defense had staked out its turf and its vision in a monograph that was well reasoned and consistent with traditional American military thought, but barely circulated to other departments of the government before it went to print.

If this line of thinking was clear (even inevitable) within the Department of Defense, it was far from so elsewhere. The Department of Homeland Security, with the statutory responsibility to defend the Nation's critical infrastructure, belatedly pushed back (or at least shifted emphasis). Lynn's counterpart at DHS, Jane Holl Lute, co-authored a piece just months later, declaring that "Cyberspace is not a war zone" and then adding that "cyberspace is a place where geography matters differently...and the role of nation states in its security is an open question."

State Department officers echoed similar concerns pointing out that the emphasis on cyber as a separate domain threatened to mute still important aspects of sovereignty and enduring principles of international conduct.

The White House quietly followed with several pages of labored prose with internal instructions on how to publicly talk about "cyber" in a way that tried to synthesize these views.

And if the rationale for and foundation of CYBERCOM created bureaucratic ripples in the United States, it had at least as powerful an effect internationally. Within months of the command's formation, a study commissioned by McAfee asked 600 IT and security professionals from 14 countries which state they feared most when it came to cyber attacks. The answer? The United States, beating out the traditional American bogeymen, Russia and China.

It's not clear if the causal relationship between the command's formation and the survey results is a tight one or if the attitudes reflected in the survey are enduring, but they do suggest the degree of suspicion that was present.

Part of that suspicion is surely due to military cyber's peculiar heritage as the child of the intelligence community. It is no accident that US CYBERCOM is collocated at Fort Meade in Maryland with the National Security Agency, America's largest espionage service. No coincidence either that the head of the Command also serves as the Director of the Agency.

This pattern is largely followed in other states arming themselves for cyber. Unlike the physical domains where reconnaissance of a target is usually a severable and more easily performed task than actually attacking it, in the cyber domain the intelligence function (penetrating a target, living on it undetected for a long period of time while extracting critical data) is actually the operationally and technologically more demanding task with the actual attack often being simply a lesser included case of the reconnaissance. Hence the tight relationship between cyber intelligence, cyber defense and cyber attack.

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

These intelligence roots give cyber a more ominous air than it would otherwise have and the phenomenon is reinforced by the intelligence community's traditional secretiveness.

That secrecy presents additional problems as the United States and other cyber-faring nations attempt to create domestic and international "rules of the road" for the new domain. Consensus on some very difficult challenges will depend on informed discussion and debate, which can only take place with a degree of transparency that is not now commonplace.

Domestically for the United States, the new domain creates seams between the Department of Defense (which technically has authority to defend only .mil) and the Department of Homeland Security (which must defend .gov and help others secure .com and similar civilian spaces). Beyond the question of creating adequate competencies in not one but two Departments, the legalistic division of the domains defies operational and technological realities.

Similarly, American Congressional oversight is divided along the traditional lines that separate intelligence from military operations, even though in this domain they are indistinguishable and inseparable.

More globally, what constitutes cyber-"aggression" remains an unanswered question. Most Americans label any unpleasant event on the Internet as an "attack", but much of this today is really cyber-espionage, the stealing of secrets through remote means. Espionage is generally considered an accepted international practice but in this domain the targets are so frequently civilian trade secrets or corporate intellectual property that the old conventions could be called into question.

And what about cyber-activity that collapses another nation's network, as Russian "hackers" did in Estonia in 2007 and in Georgia in 2008? Since much of this activity flowed through servers not in Russia but in third countries, what right did the targeted countries have to "shoot back" or at least pursue the intruders? Does a file on a server in say Houston or Bonn enjoy the same kind of sovereignty that the building or the neighborhood in which it is located does? Does the American or German government inherit some sort responsibility for allowing their "neutral" territory to be misused?

The use of cyber-tools to create physical destruction sharpens all of these questions. It now appears clear that someone used a weapon comprised of "ones and zeroes" to disable a bank of centrifuges at the Iranian nuclear facility at Natanz. As desirable as slowing the Iranian nuclear program may be, this represents the first significant use of a cyber device to create physical destruction in what another nation could only describe as its own critical infrastructure.

Nothing could put the issues surrounding cyber attack and defense into sharper relief.

The United States military was among the first to organize itself for cyber-operations. As I participated in that process – in a nation with much to lose of its treasure, privacy, commerce and security in this new domain – I knew that that was a prudent and necessary step.

But I also know that the Command's formation created and accelerated as many questions as it seems to have answered. There is much more to be resolved as we, our friends and our competitors grapple with this new dimension, and how these questions are resolved will affect us all. ■

'Our systems are targeted daily'

John Suffolk, Huawei's Global Cyber Security Officer, sees cyber security as a shared global problem and promises: 'We support international collaboration, openness and verifiable trust'

In your view as a representative of an international ICT company, what are the current challenges in the field of cyber-security?

In our view cyber-security is challenged by three main factors: Firstly, technology is developing so fast that our collective industry's ability to cater for the increasing threats is becoming harder and harder. Secondly, national borders, laws and regulations are not respected by a world intertwined with technologies and service providers from around the world. Thirdly, the industry is characterized by complex international supply chains, which increase the risk of cyber-security threats. Seventy percent of components used in Huawei equipment comes from outside mainland China making the concept of "foreign developed" meaningless.

Cyber-security is not a single country or specific company issue. All stakeholders – governments and industry alike – need to recognize that cyber-security is a shared global problem requiring risk-based approaches, best practices and international cooperation to address the challenge.

On what level – nationally and internationally – do you see these standards emerging?

All technology users and vendors have an equally large stake in finding a solution to address these challenges and we must set a better example. Industry and governments must work together to develop the right policy framework to enhance cyber-security.

We favor and support international collaboration, openness and verifiable trust as the foundation for a world where technology can continue to drive economic and social improvement for the majority of the seven billion citizens on the planet.

Governments must take the lead to establish united and integrated governance to drive forward comprehensive and collaborative approaches to cyber-security – Huawei commits itself to supporting such an endeavour.

How important is a joint European approach in terms of cyber-security?

Europe holds a unique place in the international community. Whilst it may have its challenges it is the one area where 27 countries come together under common objectives – an open market and common standards and laws. This is a wonderful platform that, if we can capitalize on it, should give Europe the ability to set standards, policies and best practice that can fundamentally position Europe as a technology innovation engine of the world.

Given that we are joined by a set of common objectives we are also joined by a set of common threats, cyber-security is one of them. The reality is: As we intertwine our services, systems and operations we intertwine the risk of cyber-security. Without being melodramatic we succeed together or we fail together.

What could effective cooperation between government and industry players look like?

Effective cooperation between government and industry means that all governments and industry must have a voice – everyone must be treated equally. We must focus on facts not fiction, we must understand the real problems, and we must ignore commentary that is meant to inflame. Instead we should focus on activities that bring parties together to forge strong open, trusting productive relationships. Achieving an effective, global, industry-wide solution is going to demand sober and fact-based dialogue, not commercial or political jousting.

How do you assess the current political initiatives to create an international accepted cyber-security framework?

We fully support these initiatives as long as they are fair, reasonable and non-discriminatory. Huawei is passionate about supporting mainstream international standards and contributes to the formulation of such standards. By the end of 2011, Huawei had joined 130 industry standards organizations in which we hold more than 180 positions.

What in particular can Chinese companies contribute in order to increase global cyber-security?

First of all the notion that companies or products from one part of the globe can be trusted more than companies or products from another part of the globe is nonsense. It is not about East or West or even North or South, it is about a global supply chain. So whether you are a Chinese company or a company from Timbuktu, you probably have a role to play in our combined challenge.

In the past Huawei was often confronted with security issues or the support of Chinese public authorities. How does Huawei answer to such accusations?

We start by explaining the facts. We operate in over 140 countries; Over 72 percent of our employees are locals from the country we operate in; 70 percent of components come from outside of mainland China and so on. Then we say "do not believe us, come and audit, inspect and verify everything we do." We believe that the best way to address such concerns is to be totally open and transparent.

How often has Huawei been targeted by cyber attacks?

We are no different to any other global leading edge technology company. Our internal systems are targeted daily with focussed attacks on our systems, and of course when you serve a third of the planets population, somewhere in the world your technology is being targeted.

How do you protect your own systems?

As a global leading telecom solutions provider, Huawei is fully aware of the importance of cyber-security.

We start from a simple premise: Assume nothing, believe no one, and check everything, and we encourage our customers to take the same approach with all of their vendors. We then take a top-down, left-to-right, right-to-left and bottom-up approach and in every part of Huawei we build in best practice for cyber-security. It is a "built-in" strategy not a "bolt-on" strategy. That way cyber-security is everyone's role, not a specific person or team's role. What is crucial is full Board support – if it isn't important to the Board it won't be important to anyone else. That is why we have a dedicated Board Committee for Cyber Security and our founder has personally published our policy on cyber-security as well.

HUAWEI

Huawei Technologies

is a Chinese multinational networking and telecommunications equipment and services company. The Shenzhen, Guangdong-based company has a turnover of €32 billion and employs 150,000 people worldwide. It recently overtook Ericsson to become the world's largest telecoms equipment maker. The company's European headquarters are in Düsseldorf, Germany. Huawei Technologies Deutschland GmbH has more than 1600 employees in Germany. John Suffolk (picture) is Huawei's Global Cyber Security Officer.

How do you ensure that your products are secure? Do you guarantee that your products and solutions are 100 percent safe?

Huawei has a proven track record of providing secure products and solutions to our customers and we adhere to stringent customer procurement and product security standards. Since our founding, there has never been a time when Huawei's commitment to security has ever been called into question by our customers. Nevertheless, there's no such thing as a 100 percent guarantee. No one promises that.

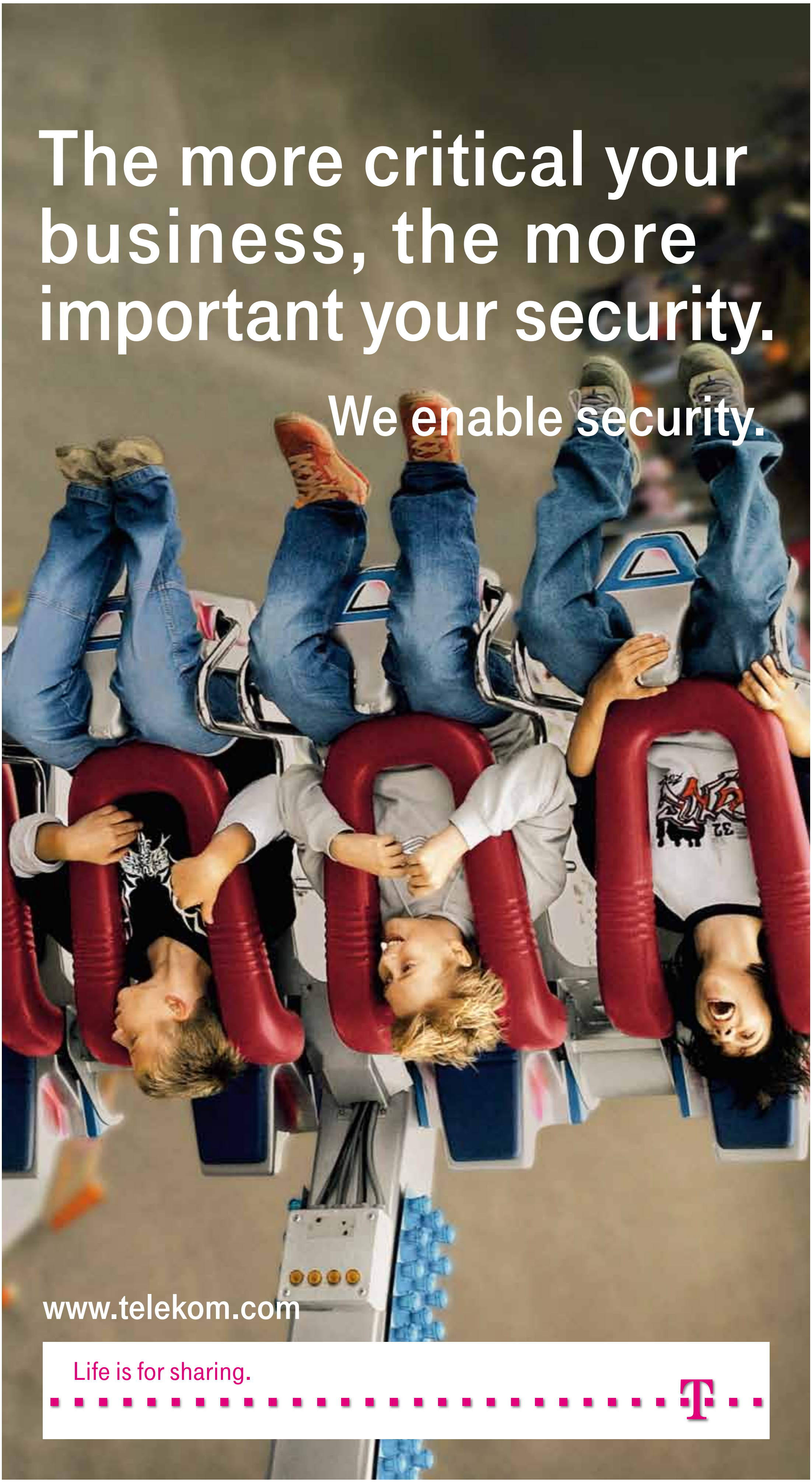
The reality is that every part of your business, and those who you take hardware and software components from, must work together to minimize the risk. We have a rigorous set of processes that we have developed with IBM since 1997. These processes enforce a systematic approach to everything we do including R&D. But given that, we make no assumptions, nor believe anyone without verification – we check the quality and safety of our products in an independent way multiple times.

We believe we are one of the few, if only, global technology companies that allows multiple organisations to independently verify our products. They apply whatever testing, reviews, methods and tools to our products – we have no say in how they do this. We believe that this unique openness, transparency and collaboration is the best way to drive up the security quality of technology products – we believe that all vendors should do this.

What is your outlook regarding cyber-security?

With the recent publications of threats such as Stuxnet and Flame, the world has reached a decision point: does it continue on its current path whereby any misguided actor, regardless of motive, can operate freely in an unregulated world and develop malware for any purpose? If we accept this route, then we must stop complaining and accept the consequences of the cyber race to the bottom of the pit and the return of the Wild West. Or should we collectively step back from the precipice, as we have done in other forms of warfare, and establish laws, norms, standards and protocols.

We favor and support international collaboration, openness and verifiable trust as the foundation for a world where technology can continue to drive economic and social improvement for the majority of the seven billion citizens on the planet. ■


The more critical your business, the more important your security.
We enable security.
www.telekom.com
Life is for sharing.