# Strategic Outlook 2013

Magdalena Tham Lindell, Jerker Hellström,
Lena Molin and Åke Wiss (eds.)

FOI-R--3682--SE

June 2013

FOI

# Strategic Outlook 2013

Magdalena Tham Lindell, Jerker Hellström,
Lena Molin and Åke Wiss (eds.)


June 2013

FOI-R--3682--SE

ISSN 1650-1942
Printed in Stockholm 2013 by the Swedish Defence Reseach Agency, FOI
FOI-R--3682--SE
Approved by Maria Lignell Jakobsson

# Table of Contents

# Preface

Since the launch of FOI's Strategic Outlook in 2009, Sweden has come to face many new challenges relating to defence, foreign and security policy. Not least since the last edition was published in June 2012, the Swedish defence policy debate has been fuelled by developments at home and abroad, and has become more intense.

The Swedish troop contribution to the NATO-led mission in Afghanistan is coming to a close, prompting questions about whether Sweden should increasingly contribute to the United Nations' peacekeeping efforts. Meanwhile, the Swedish Armed Forces are facing challenges in terms of both financing and the ability to recruit soldiers and sailors. There is a need for major, long-term commitments; the alternative for the Armed Forces is to radically lower their ambitions. Moreover, Sweden's Armed Forces must undergo the modernisation required for them to be an attractive employer.

Strategic Outlook 2013 also looks beyond the realm of strict defence policy issues and raises matters relating to public safety and security. One area that is specifically addressed is the consequences of the uninformed choices made by individuals. For example, crisis management carried out by authorities is sometimes based on assumptions about human behaviour in severe crises that has no basis in empirical data. Sweden's civil emergency planning is also discussed from a technical perspective, highlighting the vulnerability of the wireless crisis management systems that are under construction in Sweden. Moreover, as a result of our dependence on the Internet we often unintentionally share private information which can be used for mapping for commercial purposes, as well as political ends.

Where our immediate vicinity is concerned, the report this year focuses on areas of conflict between Russian politics and Islam. Russia's actions vis-à-vis Syria and Iran have aroused strong reactions both in the Middle East and among its own Muslim population. The Russian political leadership's support for Shiite actors such as Iran and the Assad regime in Syria is alienating the Sunnis, who make up the majority in Islam.

Strategic Outlook also addresses a range of international challenges, focusing on problem areas in which the international community has chosen to cooperate. One such area is the spread

of chemical and biological weapons, which could increase with the globalisation of knowledge and developments in technology. Another theme discussed is environmental crime, which has grown into the largest illegal business in the world after drugs and arms, measured in terms of financial value. Threats against global shipping and trade – e.g. smuggling, piracy and terrorism – are addressed in terms of ways to handle such threats – by way of technological progress and new forms of cooperation.

Whereas there are international regulations covering the use of the sea, the use of space is an area that is governed by a law that is in many ways outdated. This is something that the European Union is trying to address by means of implementing a Code of Conduct which aims to improve security in space.

Sweden is participating actively in international cooperation in all these areas, but also plays a unique role in nuclear disarmament where, through FOI, it is involved in the technical verification of nuclear tests. For example, in March 2013 FOI was able to confirm that North Korea had tested a nuclear device.

An issue that touches many policy areas – defence and security policy as well as foreign and trade policy – is the high-tech industry's growing demand for rare earth elements (REEs). Currently, 95 per cent of the world's rare earths are extracted and processed in China. In the longer term, industry is faced with the potential risk that it will not able to ensure the supply of REEs.

Strategic Outlook 2013 demonstrates the great diversity of issues that are of significance for national and global security. Through the selection of themes, the editors wish to present a number of security policy challenges and trends that could provide new insights and stimulate further discussion.

The editors would like to thank those who have contributed to this year's edition of Strategic Outlook, and in particular to express their gratitude to the authors.

Stockholm, June 2013

**Magdalena Tham Lindell** Chief Editor
**Jerker Hellström** Project Manager and Editor
**Lena Molin** Editor
**Åke Wiss** Editor

# The Return of the Blue Helmets? Swedish International Operations Post-Afghanistan

Cecilia Hull Wiklund, Claes Nilsson and Markus Derblom

*As the Swedish military operation in Afghanistan is being transformed, a large number of soldiers, officers and capabilities will be made available for new operations and tasks. This will result in increased freedom of action in terms of deciding how and where Sweden can best contribute militarily to international peace and security. A review of Sweden's options and priorities regarding future international operations should – alongside the EU and NATO – also include UN peacekeeping.*

## Sweden, the EU and NATO - but what about the UN?

Sweden has a long tradition of active engagement in support of international peace and security. The international operations it conducts aim to contribute to the prevention, management and resolution of crises and conflicts as well as to facilitate long-term peace-building. They also aim to promote Sweden's national security and Swedish interests. As a part of being able to contribute to new and unexpected peace- and security-related operations, the Swedish government has emphasised a policy of freedom of action. An important aspect of this policy is that Sweden can conduct international operations within the framework of a range of international and regional organisations.

After a long-term partnership, and participation in operations in the Balkans, Afghanistan and Libya, Sweden's cooperation with NATO in the area of peace support operations is well established. Sweden has also engaged strongly in the development of the Common Security and Defence Policy (CSDP), as evidenced by the fact that Sweden has taken part in all peace operations conducted by the EU since the very inception of the policy in the late 1990s. Sweden's engagement in UN peacekeeping, however, has had to take a back seat. Even though UN peacekeeping may seem a natural platform for Swedish foreign policy, over the last decade Sweden's contributions to UN missions have reached a historically low watermark. By the end of 2012, Sweden contributed 29 personnel to UN peacekeeping, about 5 per cent of the total number of Sweden's internationally deployed forces. In the mid-1990s, just before the UN mission in the Balkans

was taken over by NATO, that number was approximately 2,000 personnel – almost 100 per cent of the Swedish Armed Forces' international engagement.

Inside the UN, member states are valued in accordance with their engagement in the organisation's missions, particularly regarding troop contributions. Those states which contribute receive access to decision-making and their voices have credibility. Wisely used, this credibility can be translated into the ability to influence and strengthen the effectiveness of UN peacekeeping. Sweden's prioritisation of missions led by the EU and NATO has resulted in a reduction of its ability to exert such influence at the UN. While large troop contributions, individuals in leading positions, and a strong engagement previously gave Sweden a natural voice in UN decision-making, it is now more difficult for it to pursue issues of importance to Sweden in the area of peace and security through the UN. Sweden rarely has direct access to seats in important working groups and forums at the UN headquarters in New York and occupies even fewer seats of influence in the many missions around the globe.

Sweden will never be able to take part everywhere and evidently needs to prioritise where and how its resources will make the greatest difference. The use of available resources will also need to be balanced between international operations and national requirements. Other considerations, such as the transatlantic link and deeper European integration, naturally also shape political decisions.

The bringing home of Swedish troops from Afghanistan in 2014 provides an opportunity to reconsider UN peacekeeping as a tool for implementing Swedish policy on peace and security. The UN is unique in its international legitimacy, global outreach, broad peace-supporting capacity, and ability to support peace processes in the long term. These are the comparative advantages of the organisation; but Sweden's prioritisation of NATO- and EU-led operations over the last decade has meant a reduced experience of interacting with the UN which may result in (unintended) restrictions on Sweden's freedom of action in the future.

### How did we end up here?

Swedish troop contributions to UN missions are currently very limited. Other than the matter of resource constraints, there is also a historical explanation for this: the UN's failure in the Balkans and Rwanda in the early 1990s. The sense of a

stronger, rejuvenated UN in the early years of the post-Cold War era was soon replaced by a deep-going scepticism as regards the organisation's ability to effectively safeguard international peace and security. The UN proved itself incapable of preventing heinous crimes against humanity and the atrocities provoked abhorrence around the world. The criticism of the UN by its member states was harsh: the UN lacked a common doctrine and suffered from toothless decision-making, and the widespread differences in the training and equipment of the troop contributors severely hampered the effectiveness of UN missions. Many of the traditional Western troop contributors instead opted for missions undertaken within the framework of the EU or NATO: organisations which had developed processes for standardisation and within which the chain of command was more predictable. In addition, both the EU and NATO were developing agendas to contribute more actively to peace and security.

Like several of its neighbours, Sweden prioritised operations outside the UN framework and chose to develop its capabilities in collaboration with other European states. The experiences of the last decade have meant that operations within the framework of both NATO and the EU are largely familiar. A consequence of Sweden's choice of priorities is, however, that Sweden's ability to undertake UN operations has been weakened at both the level of the military units and the individual level. The number of personnel within the Swedish Armed Forces with experience of UN operations is steadily decreasing.

Assessing Sweden's commitment to the UN based solely on its participation in peacekeeping is too simplistic. Sweden provides extensive financial support the UN, including 1 per cent of the total mandatory budget contributions to the UN, which places it among the top 20 donors, providing some 600 million SEK annually to UN peacekeeping. In addition, each year Sweden provides several billion SEK to various UN organs, many of which are also of importance to international peace and security.

### An out-of-date view of the UN?

The notion of an inefficient UN still remains, but should be questioned and nuanced. In 2000 a panel was established to review the shortcomings of UN peacekeeping and make recommendations that would form a platform for change. The report of the panel, the Brahimi Report, has had major effects on the transformation of the UN peacekeeping system. The report launched an extensive reform process that has been continued with the so-called New Horizons Agenda, which since 2009

has promoted dialogue among member states as regards how UN peacekeeping can best be adapted to manage some of the challenges the organisation faces today and in the future. The process has generated important reforms, such as improved command and control; capstone doctrine for UN peacekeeping; the development of stronger partnerships with regional organisations; the restructuring of the UN departments for Peacekeeping Operations and Field Support; and the revision of the code of conduct for peacekeeping personnel.

Some of the reform efforts have been directed towards more efficient use of UN resources by increasing the level of cooperation and coordination between the UN's different agencies, programmes and funds. A part of this has been to adapt UN peacekeeping to local needs and long-term strategies. In today's complex conflicts, the resolution of which requires the application of a broad range of tools, there is rarely a viable alternative to the UN. Most of the UN's new peace operations are what are called multidimensional operations with a wide array of civilian and military components. Alongside military peacekeeping, these missions include, e.g., police reform, political dialogue, managing migration, poverty reduction and humanitarian efforts. The UN has developed an integrated chain of command where the highest representative of the UN in the operational area is responsible for coordinating all the instruments under the broader UN umbrella. As several other states and organisations are currently seeking to develop processes for strengthening this type of civil-military interaction, the UN has already had functioning integrated structures for several years.

Research shows that UN peacekeeping, despite its shortcomings, does in fact make a great difference and leads to increased peace and security. Multidimensional operations, which in practice can currently really only be undertaken by the UN, have been shown to dramatically reduce the risk of the return to war.

Over recent years the Security Council has provided examples of its willingness to overcome the toothless mandates that characterised the UN's earlier operations. Since the 1990s, UN peacekeeping mandates have become increasingly robust, meaning e.g. that the peacekeepers have been provided with an increased capacity to use force in carrying out their mandates. These mandates are authorised under chapter VII of the UN Charter (action with respect to threats to the peace, breaches of peace and acts of aggression) rather than chapter VI (peaceful resolution of disputes). The majority of new UN missions since

1990 have been authorised under chapter VII. These robust mandates have been developed not least with respect to the fact that the conflicts of today most often take place within states and have considerable effects on civilians. The Security Council, for example, justified the international intervention in Libya on the basis of the need to protect civilians from the ruling regime, a unique decision with potentially far-reaching consequences for future operations.

The evolution of UN peacekeeping has also resulted in mandates which span the entire board from preventative measures at the early stages of conflict to peace-building and reconciliation in post-conflict situations. The need to provide the missions with sufficient resources to carry out these more active (and in some cases proactive) mandates nevertheless remains. The active engagement of member states plays a crucial role in this.

Another important step in the transformation of UN peacekeeping has been the recognition of the importance of seeking active partnerships in conflict management. Collaboration with regional organisations adds legitimacy as well as making it possible to share costs and burdens and take advantage of each organisation's relative strengths and expertise. The UN's partnership with the African Union, the EU, NATO and the West African economic community ECOWAS has been strengthened over the past decade, e.g. through increased collaboration in conflict areas.

There is nothing to indicate that the need for UN peacekeeping is diminishing. After a great increase in the number of UN peace operations during the late 1990s and 2000s, the total number of troops deployed has remained at a high but steady level over the past few years. The geographic location of future operations may vary, alongside the extent of the operation. The largest UN mission currently deployed, MONUSCO in the Democratic Republic of Congo, is now experiencing a qualitative reinforcement. At the same time, the international community's attention is being directed towards new conflicts and peace processes. Regardless of whether future operations seek to manage the long-term consequences of negative developments (e.g. in Syria and Mali) or to support positive developments (e.g. in Somalia), there are few viable alternatives to UN peacekeeping.

### Time to reconsider Swedish participation in UN peacekeeping?

Now that Sweden has opportunity to review what instruments

best serve its national interests as well as international peace and security, there are several reasons to reconsider its role in UN peacekeeping.

**To contribute is to be there**. Robust mandates require robust capabilities. Sweden, like many other European states, has capabilities which are sought after within the framework of UN peacekeeping: helicopters, unmanned aerial vehicles (drones), Special Forces, maritime capabilities, etc., in addition to specialised competences in areas such as logistics or security sector reform. Sweden has the potential to contribute to military activities as well as police efforts or broader reform of government institutions and legislative structures. Several of the UN's missions encompass local capacity-building, a task for which Sweden has shown itself to be well equipped in missions undertaken by other organisations in countries like Kosovo, Afghanistan and Somalia. To contribute such capabilities, which are greatly in demand, would give Sweden new political leverage in the UN.

**Engagement should be based on the comparative advantages of each framework organisation**. Increasing Sweden's participation in UN missions does not mean that Sweden will need to abstain from supporting missions led by the EU or NATO. On the contrary, the different options can be seen as complementary. Peacekeeping missions are rarely undertaken in isolation from other international and regional organisations. This development is clearly in line with the Swedish view on multilateralism and an efficient use of resources. Different organisations have different strengths and weaknesses during the different phases of a conflict. Sweden does have the freedom to choose, and where the UN carries the comparative advantage Sweden should recognise and make use of the potential of the organisation. Working to bring for example the EU and the UN closer together may also result in greater synergies between various Swedish peacekeeping engagements. To enable the absorption of EU battle groups, in full or in part, into UN missions would also increase Sweden's freedom of action to make use efficiently of an advanced capability developed for international operations.

**Participation should be founded on several policy areas.** Member states that skilfully use participation in peacekeeping to complement other measures, such as development aid, achieve synergies in terms of increased effectiveness, efficiency and sustainability. The UN's breadth and stamina provide a solid platform for long-term conflict prevention and peace-building.

Prioritisation of missions should be based on the levelling of several political priorities. Can we, by initiating discussions of investment and development in relation to particular military capabilities in both foreign and defence policy circles, reach better-founded decisions? Helicopters and combat engineers are needed both for national defence and for international peacekeeping.

**A platform for Nordic cooperation?** Sweden can also work for a Nordic dimension to UN peacekeeping. The UN is the only organisation leading larger missions in which Finland, Norway, Denmark and Sweden take part under the same conditions, which facilitates deeper cooperation. Previous Nordic collaborations include SHIRBRIG, a UN-mandated rapid reaction force initiated by the Nordic states. A Nordic platform in UN peacekeeping would provide greater political leverage and offer an opportunity for burden-sharing at the same time as the states could jointly offer a substantial, interoperable contribution to peacekeeping.

In general, the UN has the breadth and approaches needed to realise the objectives of Swedish foreign and defence policy. The UN is also undergoing a reform to better meet the challenges of the 21st century. Important aspects remaining include the development of the Security Council; the still remaining gap between mandates and resources; the development of troop generation processes and increased predictability of contributions; and continued development of military command and control. If Sweden wants to influence the reform process, an increased and more active participation in UN peacekeeping will be required.

## Further reading

Derblom, Markus; Hagström Frisell, Eva; Schmidt, Jennifer (2008) *UN-EU-AU Coordination in Peace Operations in Africa*. FOI-R--2602-SE.

Nilsson, Claes; Zetterlund, Kristina (2011). *Arming the Peace: The Sensitive Business of Capacity Building*. FOI-R--3269--SE.

# Defence Capability with Impediments – Defence Economic Choices Facing the Next Strategic Defence Review

Mikael Wiklund

*Sweden is currently facing one of the largest challenges in the area of defence economics ever. After years of facing low political interest in defence-related issues and a politically declared "strategic time-out", the Swedish Armed Forces have recently declared – in the midst of the current defence reform – that their budget is insufficient for the arrmed forces to be operationally relevant. According to the Swedish Armed Forces, the shortfall over the next ten-year period exceeds 50 billion SEK. The alternative to providing this additional funding is to radically alter the ambitions. How did this happen? And what are the most important choices facing Sweden?*

The debate about the Sweish Armed Forces long-term financing recurs frequently. Any new strategic defence review is usually preceded by, and may be motivated by, problems in achieving political ambitions within the assigned means. An open political conversation regarding the economic position of the SwAF has been on-going in Sweden ever since the Supreme Commander made the statement at the Annual National Conference of Folk och Försvar (Sociely and Defence) in 2011 that "the current economic conditions are insufficient for implementing and maintaining the future operational organisation (Insatsorganisation 2014) in the long term". Ahead of the 2013 Conference, the Supreme Commander also stated in an interview that the operational organisation that the defence reform aims to realise can only be sustained for one week should Sweden face even an attack against a limited target. For the first time in years, this has brought the area of defence into the political foreground and into central areas of media reporting. In late February 2013, the SwAF presented, in a report to the government, their view on future developments and the preconditions for economic balance in the long-term.

## The defence reform encounters problems

The 2009 Defence Decision and the government's strategic decision concerning the SwAF for the years 2010–2014 gives the impression that the Operational Organisation 2014 would in fact be in place by the year 2014. The implementation was, nevertheless, conditioned

by the term "at the pace permitted by the current budget". The initial ambition was adjusted early on, as the SwAF conveyed that the new structure could really only be fully implemented by 2019. In the February report, the SwAF assessed that the imbalance in the production of military units would amount to some 1.3 billion SEK annually. The additional needs related to materiel procurement were calculated at approximately 51 billion SEK up until 2023. However, the SwAF currently only carries capacity to manage about 31 billion from the point of view of ordering and receiving materiel – meaning that, even should the imbalance be filled, the SwAF would not be able to be operationally relevant even by 2023. How did this happen?

The reasons are numerous. Some of the most important, which can be identified in the SwAF's report, are: too optimistic planning assumptions; reforms that did not free-up resources at the anticipated pace; limitations due to political management and control of peacetime organisation and production conditions; and price escalation that is not compensated for or is undercompensated. The government's principles for materiel procurement, the strategy for materiel procurement, and requirements concerning economic balance have also entailed that renewal of military materiel has been pushed into the future, resulting in increased operational costs. In sum, the SwAF declare that "the long-term expenses of the defence reform have been underestimated". In addition, several political decisions have been made which increase the strain put on the SwAF's budget – purchases of the HKP 16/Black Hawk helicopter and the next-generation fighter aircraft JAS 39 E, for example.

Which then are the most central issues that need to be addressed to generate the conditions for a balanced defence economy, and which decision points are we currently facing? The most central issues are not exclusive to Sweden. In the light of the current economic crisis and a diminishing willingness to spend resources on defence-related investments, a similar discourse is taking place in e.g. the UK and the USA. Any state wishing to maintain a functioning defence policy over time needs to make some important choices: how should the necessary effect of political directives be achieved? How should resources be divided between short-term deliveries and long-term capacity/relevance? How should price escalation and demands on productivity be managed? Which operational risks are acceptable to reduce cost? What collaboration can or should be entered into? In Sweden, these have been addressed as follows below.

### Weak effects of political management begets the need for detailed policy control

In Sweden, the area of defence has experienced a long period of restructuring, but the effect of the political management has often

been weak. A number of inquiries and reviews have been undertaken by the government since the turn of the century. These have come about due to a perceived lack of insight into and control of the on the part of the government. The SwAF are regarded as often revising previous assumptions and forecasts; being slow-moving on issues relating to internal structural reforms; providing feedback that is difficult to interpret and to trace over time; and as having challenges in clearly tying the need for resources to demands for results. The large number of inquiries and reviews is likely an expression of the fact that both the Parliament and the Cabinet are not experiencing the anticipated effects of political directives, alongside difficulty in evaluating the SwAF's work.

The government is at an information disadvantage in relation to its civil service. This control problem often means that the government has to choose to be passive or to exercise a control that is profound and more detailed than what is customary in the Swedish public administration. From time to time the government has chosen the latter. The advantage of this is that it enhances the government's control on a range of issues by direct management of areas such as organisation, the SwAF tasks and responsibilities, major defence systems and number of employees. The downside is that micromanagement creates significant disadvantages. Among other things, it creates a great need for analytical skill to determine the effectiveness of policy, and there are obvious risks of a lack of a holistic approach. The main drawback is that it could also be interpreted as the government indirectly taking over responsibility for results from the SwAF and that failure can always be blamed on the government's "meddling". This could lead to a confusion of roles between the Cabinet and the SwAF and the responsibility for failure can then be laid on the Cabinet and the Ministry of Defence.

### Financial balance at the cost of diminishing long-term capability?

Today's equipment, technology and knowledge are the result of historical investments. There is always a temptation in times of economic challenges to borrow from tomorrow's relevance to handle today's problems. The SwAF reform and economic balance of the SwAF have largely been financed by the postponement of planned materiel acquisition and reductions in research and development (R&D) and a lowering of ambitions. Funding for R&D has fallen by about 40 per cent between 2008 and 2013 (from 1.05 to 0.62 billion SEK). The corresponding figure for the funds for materiel procurement and support is a reduction of approximately 10 per cent (from 17.2 to 15.5 billion SEK). The trend is even stronger if price escalation is added. This means that the fulfilment and establishment of military units today have been at the expense of future capability.

The trend is not sustainable in the long term. The SwAF indicate in their report that short-term economic considerations have forced major equipment needs to be postponed into the future. Sooner or later, these needs have to be satisfied if the SwAF's work is to remain militarily relevant. At the same time future military activities are predicted to become more knowledge- and technology-intensive (compare the development of the cyber area, unmanned and autonomous vehicles, space, network-based information sharing between sensors and weapons, etc.). This suggests that R&D and equipment should be given a higher, rather than a lower, priority.

### Today's demands for productivity reduce effects, and create weak political traceability

The defence area is associated with particularly difficult conditions in making its operations continuously more efficient. Among other things, this is due to high fixed costs and slow movement in switching production; poorly functioning markets on which the SwAF gets its resources; little opportunity to replace different inputs with each other; personnel as both input and output; major limitations on the degrees of freedom due to high demand for political control of the production and the fact that the effect of the SwAF decreases with the development of prospective adversaries. The demands made on the SwAF do not take these limitations into account. The trend is rather the opposite. Demands are – perhaps unconsciously – stacked upon each other partly through the yearly wage and price conversion; targeted policies and streamlining aimed at redistribution or reduction of funds; and the rising cost of defence equipment that outstrips the compensating funding.

Difficult conditions in combination with the demands put upon them are creating economic deficits in the SwAF's operations. These deficits can only be tackled by opting out of activities or obtaining additional funds. Much of the reductions of funding that have been promoted as efficiency improvements in recent years are most probably in practice to be regarded as mere reductions in effect. Such effect reductions, provided they are in line with the political will, should be done in an orderly and conscious fashion.

It is also important to note that the most important and long-run sustainable source of productivity – based on economic theory – is knowledge. In our context, this consists of investment in the development of doctrine, concepts of capability, production, and R&D. The knowledge also needs be incorporated in military units through the introduction of new tactics and doctrine, better equipment and new ways to practise and train. The military history of productivity consists almost exclusively of the introduction of new technologies and doctrines. The redistribution of funds for

knowledge development to the production of military units can be expected to have consequences in the form of significantly lower productivity in the future.

### There is a risk that today's financial balance has been created at the cost of higher operational risks

There is often a trade-off between risk and resources. Large stocks of strategic goods, units in high readiness, investments in knowledge, modern equipment and the domestic supply of military equipment are all examples of factors that reduce operational risks and provide strategic freedom of action over time. The drawback is that they are costly. There is therefore an obvious risk that financial balance has been achieved at the cost of increasing operational risks – perhaps in the form of small stocks of expensive ammunition, ageing equipment, reduced R&D and capability mismatches between "tail" and "teeth" in military units.

Excessive cost-cutting leads to operational risks and deficiencies in the strategic freedom of action. Conversely excessive risk aversion leads to unacceptable costs. To design for complete options in various technical systems is expensive and probably means that the majority of the options are never triggered. At the same time, options can avoid costly new acquisitions and provide opportunities for worthwhile extensions of the lifetime of equipment.

### Sweden needs to tie the design of the armed forces more strongly to the choice of forms of bi- and multilateral cooperation

The rising cost of defence equipment and dwindling resources make collaboration with others increasingly important. Working together with others has important advantages. Together, one can achieve better economies of scale, exploit comparative advantages, establish a niche or carry out joint technology and capability development. Looking at the development of advanced weapons and weaponsplatforms, we are approaching the time when it is going to be, economically, nearly impossible to act unilaterally – especially for a small country like Sweden. Bilateral or multilateral cooperation may soon be the only way to get early access to advanced military systems. Likewise joint capability or capability development could give Sweden access to benefits that one would otherwise have to allocate more resources to or renounce all together.

Working together with others also has important downsides. It takes longer and creates more administration, forces sacrifice of own requirements and builds dependencies. Technology, knowledge and capabilities are also national resources whose exclusivity serves a purpose in itself. In addition, sharing capabilities will only work

as long as not all partners request a capability simultaneously – a situation that might arise should there be a deterioration in the international climate. In such a competitive situation, with a scarcity of resources, Sweden may, all too late, find itself last in line.

It is also important to note that the step from joint capability development – including the development of equipment and doctrines as well as combined exercises – to mutual defence obligations is not a very big one. In a situation where Sweden abandons qualified capabilities for those of another state, the step has in fact already been taken.

The choice of collaboration must therefore also be a choice of the broader design of the SwAF. The main issue is not just how much resources should be spent, but also how they should be distributed for maximum benefit. Collaboration requires that resources be allocated to ensure that Sweden is an attractive partner. The recent development of redistributing funds from the area of R&D in reality means that one of the few – and relatively cheap – advantages that Sweden has to offer to defence cooperation is being eroded. Generating a similar international appeal based on operational capacity rather than R&D is many times more costly.

### Being relevant or just being – the difficulty increases

It will probably cost more to produce the Operational Organisation 2014 than can be afforded within the means assigned. The defence debate and the issue of the SwAF's finances can nevertheless not be reduced to a question of how much funding the SwAF should be given. How to achieve balance and make difficult prioritisations is at the centre of any defence economic discussion. A discussion of future armed forces in balance should be based on a genuine understanding of what the situation concerning the issues addressed in this paper looked like during the 2000s and how we anticipate that it will look in the future. Otherwise the risk is that any new discussion on defence economics will generate continued imbalances. In the short term the issues rest with the Swedish Defence Commission (Försvarsberedningen). In the long term the responsibility is shared between political representatives and the management for the next strategic defence review. Only when we know how Sweden should relate to these different choices can we really ask the big question – what can defence be allowed to cost?

# Who Wants to be a Soldier?

Malin Ivarsson and Amanda Eriksson

*On 1 July 2010 Sweden went from a conscription system to all-volunteer armed forces. A large number of soldiers and sailors are now to be recruited from the labour market. What are the implications of this for the Swedish Armed Forces? Today's high youth unemployment in Sweden can be viewed as an advantage here, but most of the challenges lie not in the present but in the future – a future characterised by an ageing population, an increased demand for manpower and generations who have limited or no experience of the military. What can the Swedish Armed Forces do to deal with the future challenges associated with the transformation to an all-volunteer force? Now is the time to cast light on to these questions, for what are the options – an armed force without soldiers and sailors?*

## From conscript to all-volunteer

On 1 July 2010 compulsory conscription for men in Sweden in peacetime was suspended. Voluntary basic military training named *Grudläggande militär utbildning* for three months replaced the old system. After the training, recruits may apply for a time-limited employment for a maximum of 12 years in the Swedish Armed Forces (SwAF). Soldiers and sailors with time-limited contracts are not a new phenomenon in Sweden. Such contracts existed under the conscript system, but with a limited duration of two years which then automatically became a permanent position.

One major change resulting from the transformation of the system for manning the armed forces is that there are now two forms of employment for soldiers and sailors – regular servicemen and reservists. The main difference between these two types of service is that the reservists have their principal employment with an employer other than the SwAF. The Swedish Armed Forces estimate that by year 2016 they will need to enrol 5,500 persons in the basic military training. These estimates are based on an assumption that the regular serving soldiers and sailors will stay on average six years. If this assumption is not fulfilled the consequence will be an increased need for recruitment.

The transformation from a conscript to an all-volunteer force entails more than just different lengths of contract and shorter basic military training. It means that the Swedish Armed Forces will have to compete with other employers for manpower

among a fairly young workforce which not has been introduced to the military in the same way as previous generations of men were through conscription. What are the main challenges the Swedish Armed Forces are facing due to the change to an all-volunteer force and what can the organisation do to manage these?

### Difficulties in recruiting and retaining personnel

Youth unemployment is currently high in Sweden, even in comparison with other European countries. This can be considered beneficial for organisations which need to recruit young personnel in large numbers. But what happens when the economy recovers and unemployment falls? The armed forces' needs to recruit will be the same regardless of the state of the economy. The armed forces must also attract a target audience with different educational backgrounds in order to meet the needs for both soldiers and officers.

The young generations of today move between employers more than previous generations did. This is partly beneficial for the Swedish Armed Forces as the soldiers and sailors will have a time-limited employment contract, but it also involves a risk of younger personnel leaving too early. The six years that the Swedish Armed Forces are assuming soldiers and sailors will stay on average may seem like a short period of time, but for a young person in his or her twenties a great deal can change during this time frame. If soldiers and sailors stay for less than six years, this will mean even larger recruitment needs and increased costs as a result.

Like many other European countries, Sweden has an ageing population. As average life expectancy increases faster than the birth rate, the competition for manpower increases. Developments on the labour market in combination with demographic changes are changing the conditions for many organisations which need to recruit in large numbers, like the Swedish Armed Forces. Another aggravating factor for the Swedish Armed Forces is the attitude of the public and in particular the attitude of young people towards the SwAF. The report *När kriget kommit – Svenskarna och den nya försvarspolitiken [When War Arrives – The Swedes and the New Defence Policy]* (Ydén and Berntsson 2012) emphasises that the Swedish public's opinion of the Swedish Armed Forces is lower than its opinion of other public authorities. Who wants to start working in an organisation that lacks support in society?

The conscription system offered an opportunity for the armed

forces to show some parts of the public what they were doing, as young men were forced to try life in the military. The consequence was that even young men with no interest in or knowledge of the military were introduced to the armed forces, and one result of the conscription system was that the public had a better knowledge of the armed forces than it does today. When conscription started to be phased out and the number of young people enrolled decreased in the early 21st century, up to its suspension in 2010, much of society's knowledge of the armed forces was lost.

To be in the public eye is important for countries with an all-volunteer force, where only a small fraction of the population have experience of the military. When only a small fraction of the population have a direct link to the military, a potential civil-military gap might arise between society's and the armed forces' view of military activities. The result would be a loss of understanding in the public for the military (Dandeker 2010).

Today new and different methods are required to attract young recruits. The Swedish Armed Forces have to be perceived as an attractive employer not only by present-day young people but also by those that already have been recruited. Their experience has to match the image that is marketed. As their future needs to recruit are large the Swedish Armed Forces also have to attract new groups that hitherto have not felt themselves to be or have been addressed by the military, for example women. When the target audience has neither knowledge nor a high opinion of the Swedish Armed Forces, employment in the armed services becomes a marginal option.

In Sweden a majority of the servicemen and -women should be reservists. This is a relatively untested alternative and thus involves a high degree of insecurity. Reservists have their principal employment with an employer other than the Swedish Armed Forces but are sometimes on leave in order to work in the SwAF. This solution may seem like a good option for the armed forces as it enables flexibility in the workforce, but how good is it for the principal employer?

In order to succeed the reserve system requires that the principal employer feels that there is an additional value in employing a reserve soldier or sailor. A consequence of the decreasing knowledge of the Swedish Armed Forces among the public is that recruiters in other organisations will also not know enough about the armed forces or about what someone with a background in the armed forces has to offer. To get people to

choose to become reservists, the additional employment as a soldier or sailor must add value and not make it more difficult to find a principal employer. The present low level of faith in and knowledge of the Swedish Armed Forces among the public is a challenge.

### Why is Sweden different?

Sweden is neither the first nor the last country to have an all-volunteer force. The United Kingdom, the USA and Canada all have a long tradition of an all-volunteer force. There are of course lessons to be learned from these countries, but the differences in culture, labour legislation and entry requirements of recruits make comparisons difficult. In other countries that have an all-volunteer force, breach of contract is associated with sanctions. This is a big difference compared to Sweden, where the soldier or sailor can resign at any time regardless of time of contract left.

The cultural differences between the countries should also not be underestimated. In countries with a long tradition of an all-volunteer force the public have more experience of reintegrating former military personnel. This is an experience Sweden has only in part, with the reserve officers. The standards required of recruits are another field where Sweden deviates from many other countries, where standards are relatively high in comparison. Higher entry requirements when recruiting affect who is interested, the size of the recruitment pool and in the end the quality of the personnel. The United Kingdom, which in comparison with Sweden has lower requirements when recruiting, emphasises the quality of soldiers as one of the largest problems (Dandeker 2010).

These differences between the countries should not be underestimated when making comparisons. The Swedish solution whereby the majority of soldiers and sailors should be reservists is quite unique, which makes it even harder to find countries with which comparison is relevant or illuminating.

In United Kingdom, the armed forces have succeeded well in creating support among the public. In a survey regarding the public's opinion of the British Armed Forces, eight out of ten respondents have a high or very high opinion of them (Gribble et al. 2012). Here it can be of interest for Sweden to study how the United Kingdom has worked to highlight the armed forces' work in wider society.

## What are the challenges and what can the Swedish Armed Forces do?

The Swedish Armed Forces today face significant challenges in the supply of personnel, but the situation is most likely to become even more challenging in the future. An ageing population and increased competition for labour are parameters that the armed forces authority cannot affect. What it can affect, however, is how it chooses to respond to these challenges.

Another question is why the public in general has such a low opinion of the Swedish Armed Forces. Is this low opinion a sign of lack of knowledge of what the armed forces do? When only a small fraction of the population have any knowledge of the armed forces, their need to be seen and to be seen in the right way in society, in order to improve the relationship between the military and the public, increases. To attract young people to the basic military training the SwAF have spent a great deal of money on advertising campaigns. The campaigns have been highly acclaimed by professionals, but have they contributed to a more positive image of the Swedish Armed Forces, when the same authority at the same time is involved in a public debate concerning financial inefficiency, soldiers' pay and the lack of capacity to defend the national borders?

In order to keep the soldiers and sailors they recruit, the Swedish Armed Forces not only have to be viewed as an attractive employer, they also have to be an attractive employer. Recruiting contract servicemen and -women who are there of their own free will is a major cultural and mental change for the SwAF. Changing the culture of an organisation usually takes time – time that the Swedish Armed Forces do not have. The question of how to retain the labour force will in the future be as important as how to recruit it.

In the end it is all about creating trust and support among the public for the work the military does. This might require the Swedish Armed Forces getting into the public eye in order to legitimise and create an understanding for their work. The lack of knowledge among young people of what it really means to be soldier or a sailor means that the visibility of the military's work and the profession is one of the most important questions. If the target group does not know what the armed forces do then the military is not likely to be a real professional alternative. It is also important that the image projected by the armed forces reflects the reality so the young persons' perceptions of the military not are based on action movies.

Both in recruitment and in the process of retaining personnel it is important to look for long-term solutions, as the Swedish Armed Forces cannot enforce sanctions when contracts are breached, as many other countries with an all-volunteers force can. Two easy and simple ways to attract more people are to raise pay or to lower the entry requirements. But what are the long-term consequences of such a decision? Does higher pay or lower entry requirements raise the public's opinion of the armed forces? Probably not, but there will be a larger pool of possible soldiers and sailors to choose from. Which leads to another conclusion – that the Swedish Armed Forces also have got to reach out to women, a group that has long been excluded and therefore has even less knowledge of the Swedish Armed Forces than men.

For the Swedish Armed Forces to be able to attract young people into employment, young people will have to feel that they will get something out of it and it will be a positive point on their CV. For example, employment as a reservist gives an added advantage, an additional merit when applying for positions with other employers. The value to a person's CV of having worked as a reservist must be clarified and communicated to both the target audience and other future employers. Sweden is not the first, and will probably not be the last, country to undergo changes in the supply of personnel for the armed forces. But Sweden is different from the other countries, primarily in two ways. First, there are no sanctions when breach of contracts, which means that retention is as an important question as recruitment for the Swedish Armed Forces. Second, the majority of the soldiers and sailors should be reservists and have their main employment at another employer. These differences mean that an all-volunteer force in Sweden is associated with larger challenges than an all-volunteer force in many other countries. But what Sweden can learn from other countries, such as the United Kingdom, is how to highlight the work of the Swedish Armed Forces in order to increase the public's support and opinion of the organisation. However, the SwAF must also ask themselves why the opinion and support is low, and then act on the answer.

The change from a conscript to an all-volunteer force is more than just a change in staff recruitment. It involves a significant mental shift for the entire Swedish Armed Forces. The staff supply system has already been replaced; now the organisation must undergo the modernisation necessary for the SwAF to be an attractive employer and convey this to the current and future young people and to the public at large. For what is the alternative – an armed force without soldiers and sailors?

## References

Dandeker, C. (2010) "Recruiting the All-Volunteer Force: Continuity and Change in the British Army, 1963–2008", in Stuart Cohen (ed.), *Israel's Armed Forces in Comparative Perspective: The New Citizen Armies*. Routledge, pp. 32–47.

Gribble, R. et al. (2012). *"Armed Forces"*, in *29th British Social Attitudes Report*. London, National Centre for Social Research, pp. 138–154, available at http://bsa-29.natcen.ac.uk/read-the-report/armed-forces/introduction.aspx, downloaded 20 March 2013.

# Human Behaviour in Crisis Situations – Facts and Fiction

Misse Wester

*The attacks in the USA on 11 September 2001 are sometimes used as examples of how individuals behave during a major crisis. We have all seen images from that day, showing individuals jumping from windows at a great height and falling to the ground without any reasonable chance of survival, while others ran from the collapsing buildings covered in dust and ash. The media reported on firefighters and police who went into the buildings to help others but were themselves trapped and died. What we as individuals think about how people behave during major incidents or crises is often quite different from what they actually do. There is a discrepancy between what we think was happening and what the person's intention actually was. What consequences does this have for crisis management?*

Occasionally we see a person doing something that seems illogical. If I see a person who is behaving strangely, perhaps someone who wanders back and forth, apparently not knowing where they are going, I may conclude that the person is lost. Likewise, I can infer that a person who has to evacuate a burning house has been struck by panic when I see that person running back and forth between the desk and the door, but not getting out. The same thing might happen when we see a picture on the TV news of a person running from a disaster area with a flat-screen TV under his or her arm. I may conclude that there is widespread looting in the area. However, in truth this might not be the case. A person who wanders around appearing to be lost or confused might simply be a person who is totally engrossed in their own inner world. The same might be true for the person who runs back and forth in their office; he or she might have forgotten their phone and run back to get it, then remember that her wallet is still there and go back to pick that up as well. A person who seems to be breaking into a house to rob it might just as well be the homeowner her- or himself who comes home to ensure the family's belongings are safe or perhaps to move them from one place to another.

If I, in my capacity as an ordinary citizen, interpret the world based on what I believe and draw incorrect conclusions based on those beliefs, it makes no difference in my everyday life. However, this kind of misinterpretation can cause problems in a disaster situation. For example, when hurricane Katrina was approaching New Orleans the inhabitants were reluctant to leave their homes for fear of being looted. As a result many people were stranded in the

subsequent flooding. The decision to evacuate or not depends largely on the trust people have in the organisations that are responsible for crisis management. If those affected do not trust the organisations responsible for temporary shelters and other housing facilities they will not use them, but will resolve the situation in other ways. This results in empty or underutilised shelters, which is not particularly resource-efficient as it involves a cost: resources could have been used elsewhere.

If the assumptions crisis managers and policymakers use to predict how people will behave lack a factual basis, there may be devastating consequences for crisis management as a whole, particularly in the preparations being made. There are a small number of Swedish studies which examine the perceptions that exist among decision makers and crisis managers about how people will behave in a crisis. The results of these studies show that crisis communicators believe that the population living in their municipality will panic to a great extent, and behave irrationally and illogically. This obviously affects the preparations made before any incident. If I as a communicator believe that my community will react with panic, it is very likely that I will adapt my communication to reduce the risk of this happening. The question then is whether the information provided is truly relevant to the audience the information is intended to reach.

An example of communication with target groups can be seen in how authorities and scientific experts chose to communicate risk in connection with the earthquake that occurred in 2009 in the village of L'Aquila in Italy. This event presented a golden opportunity for scientists to urge residents to evacuate the area, which was threatened by severe earthquakes. Instead scientists toned down the danger, which resulted in 398 fatalities. Six scientists and one government official were put on trial for involuntary manslaughter, and were found guilty in 2011. This tragic example shows that communication based on what individuals will do is essential in emergency situations and that it must be built on facts, not assumptions about how the information may be received. If the scientists had presented the information they had and the known uncertainties of this, the population would have taken a decision based on the available information. Unfounded speculation as to how information may be received may lead to the data being downplayed or even not published, which is not a good foundation on which to build credible communication with the affected community.

### Actual behaviour

But how do people really react when something actually happens? Will a person flee from danger in order to save her or himself, will he or she panic and act irrationally, or perhaps freeze and do nothing?

There is a behavioural research tradition that seeks to understand, explain and predict human behaviour during disasters where the results are not at all consistent with the image of individuals as selfish, panicky or irrational. For example, studies conducted at two of the largest fires in the United States – the fire at the Beverly Hill Supper Club in Kentucky in 1977 and the fire at the Station nightclub in Rhode Island in 2003 – showed that individuals stay together in social groups and that this affects the evacuation.

In evacuations, it is rare for people to move one by one and get out in an orderly manner. Rather, people stick together as a group – it is simply not possible for someone to flee and leave without everyone they went in with. This means both that the evacuation is slower because time is spent waiting for other group members, but also that planned evacuation routes do not work well because they are not designed for several people to get out simultaneously. These studies show that there are social ties that hold us together and the larger the group to which we belong, the greater is the risk that we will not escape the danger in time. Nor is this desire-to-help behaviour limited to one's own group: it extends to warning others and in many cases trying to help rescue workers to evacuate more people from the crisis area.

This behaviour was observed in connection with the bombings of the London Underground in 2005: the media reported on panic in the underground, but interviews with those directly affected show that, on the contrary, people helped each other with everything from comforting those who were distressed to sharing bottles of water. After the terrorist attacks in Norway ordinary citizens contributed significant help in taking care of injured both in Oslo and on Utøya. This behaviour can also be observed in the immediate aftermath of earthquakes where those who live or find themselves in the area are the first to begin rescue or searching for survivors, in most cases without formal training or the necessary equipment.

Looting in emergency situations is an unusual phenomenon, even if the impression conveyed by the media is quite the opposite. There are very large differences between the media representations of people's actions in Haiti after the 2010 earthquake and how the Japanese population – who suffered a similar disaster in 2011 – acted. In Haiti, the media described a state of looting and violence in which thefts and murders were everyday occurrences. The disaster in Japan, however, was presented in the media as an orderly situation where citizens stood in line and calmly waited their turn. Also in New Orleans the media reported that in the aftermath of hurricane Katrina there was violence, in particular inside the large sports arena where evacuees gathered. If the authorities and decision makers in these

contexts rely on media reports and believe that the image portrayed is representative of the public at large this will result in efforts intended to satisfy the perceived, rather than the real, needs of the population.

Again, it is easy to draw hasty conclusions based on the images relayed from disaster situations. Observations of alleged robbers in New Orleans show that the bulk of what was stolen was essential supplies in the form of food and water, not luxury items such as televisions or computers. Nor can actual cases of looting or murder be found in the subsequent police reports, giving an indication that such media reports are exaggerated. However, it should be noted that there are significant differences between Japan and Haiti not only during the state of emergency, but also under normal conditions. This obviously affects disaster preparedness in general and what resources are available in an emergency. If state aid efforts are started quickly and satisfy the needs of citizens there is no need to break in and steal in order to secure the essentials for survival. However, if state or regional support is inadequate, people will be forced to take other measures to ensure that their families will stay alive – but not at the expense of the survival of others. People do not normally steal from their neighbours but rather share with others the few resources available in their vicinity.

### Evidence-based crisis management

In general crisis management attempts to predict and plan for the unpredictable. In this planning we have to rely on models, hypotheses, and sometimes pure guesswork. This applies especially to human behaviour. Of course it is difficult systematically to study how individuals behave in crises because researchers are rarely there when something happens. This means that it is even more important that available knowledge is actually used in the best way.

What are the consequences for society's crisis management if it is based on incorrect assumptions about the public and the citizens? In the acute phase, crisis management may counteract our natural impulses to share with and to help others, which in turn leads to frustration which may aggravate an already stressful situation. If the crisis management plans are based on false assumptions, for example by imposing a curfew following a natural disaster in order to minimise looting, this will undermine the patterns of human behaviour that have been observed in most disasters: people organise themselves into social groups which share resources, at least in the initial phase of the crisis. In all crisis management, both domestically and internationally, the term "command and control" is used, implying that a crisis should be controlled and those affected viewed as victims and not as assets. This means not only that the crisis management might be planned based on false assumptions, but also that the inherent potential of citizens is not exploited to the full.

Being able to predict human behavior with 100 per cent accuracy is impossible and perhaps one should not expect that all citizens can be seen as a resource in a crisis. However, research shows that individuals behave predictably to a very high degree – so high that one cannot dismiss these patterns or expect that they are temporary or unique to a specific situation. These research results need to be included in modern crisis management so that it is based on facts. What is needed is crisis managament that is more firmly based on systematic observations, an evidence-based approach where crisis management is based on scientific evidence, so that the response meets the needs the citizens actually have rather than assumptions about them.

## Further reading

Wester, M. (2011) *Fight, Flight or Freeze: Assumed Reactions of the Public during a Crisis*. Journal of Contingencies and Crisis Management, 19(4),pp. 207–214.

# Privacy on the Internet – A Public Question

Steven Savage, Ulrik Franke and David Lindahl

*Modern Internet-based services are used in many ways. We work, do business, exchange news and access government and local authorities through the Internet. The downside of the Internet is that we can be monitored, cheated or stalked, suffer theft and be libelled. How does the relationship between the consumer, commerce, technology and the law work? When will we achieve the Internet's full potential? Can technology be, or be made to be, neutral?*

We all value our privacy and integrity. Nonetheless we give this different priority depending on our culture and the actual context. In contacts with our doctor, our lawyer or our priest we expect absolute confidentiality. In other situations we are often prepared– without much pause for thought – to allow insight into our private affairs in exchange for convenient services such as paying bills, online purchasing or reading the news from an online newspaper or magazine. However, the digital communication technology which makes this possible has been driven mainly by technical and commercial forces. Because of this it is difficult or in practice impossible to control what information we give away. Personal information is saved and analysed by different actors at different stages of an activity. In most cases this is done for entirely legitimate reasons such as personalised special offers or individual services, but the information can equally well be (mis)used for other purposes such as registering one's political leanings, gender and finances. Recently Cambridge University scientists demonstrated that it is possible to deduce individual persons' political leanings with a high degree of certainty simply from their "likes" on Facebook.

## Digital communication – possibilities and limitations

Decentralisation is an important factor which makes Internet-based media unique. We can all produce, consume and distribute information – simultaneously! This is in contrast to traditional media such as newspapers, TV and radio which in the main allow only one-way communication. The consumer gains a great deal by decentralisation. News is distributed very rapidly since everyone, not only journalists, can report events in real time. At a later stage the different sources can be collated and analysed. In this way different sources can be compared and biased reporting is easily detected by citizen journalists. In a democratic society this is a natural aspect of freedom of speech, whereas repressive regimes see this as a threat which challenges their monopoly on information.

The Internet's global range also reduces the importance of geographical boundaries and limitations of distance. Lobby groups or political movements can be organised and act in many countries without ever actually meeting physically. Groups without a formal structure and leadership such as Telecomix and Anonymous are current examples. Compared to traditional groups these are extremely quick to organise and very difficult to gain insight into. Because social media use the same communication infrastructure as the authorities and commerce it is difficult for a regime to close down the network. During the 2011 revolution in Libya the telecommunication network was never closed down, despite it being used by anti-government forces – in all likelihood because the regime was also dependent on the network. The economic damage suffered by Egyptian society when President Mubarak ordered the network to be closed down in 2011 has been estimated to be 90 million dollars.

At the same time Internet-based social media have disadvantages compared with other communications media. The vast majority of social media users have little understanding of how information technology works. Everyone writing a postcard is normally aware that it can be read by others between the sender and the intended recipient, whereas Twitter and Facebook users seldom or never understand how their messages are stored and transmitted. They are therefore poorly equipped to understand how and where their messages can be tracked, saved or intercepted. As a consequence the typical user has little chance to prevent tracking and interception. Knowledge is a precondition of deliberate use of safety precautions.

Another disadvantage is that the Internet is necessarily built to enable tracking and interception. This is sometimes deliberate – digital telecommunications nodes are built according to international standards which allow police and security agencies with appropriate authority to intercept communications to and from those suspected of illegal activity. The Internet is constructed so that normal traffic always contains the origin and destination of a message. Traceability is the norm.

The main disadvantage, however, is that technology allows automated searching through enormous volumes of digital data with very little effort. This allows government authorities, companies, criminals, foreign states and simply curious people to search through any information they can access. Via keywords, name of (or IP-address of) the sender, destination and the type of traffic it is possible to search through large volumes of information in search of whatever one is interested in. Only after considerable (but cheap and easy) automated sieving is there a need for a human operator to intervene. There are no comparable physical search techniques with the same

power. As an example, Syrian dissidents reported that during interviews they were confronted with reams of data logs which the regime had intercepted from their Internet activities.

Is it possible to protect one's privacy on the Internet? There are already methods which hinder tracking and encryption which prevent the contents of a communication being disclosed. However, the typical user lacks sufficient understanding of the technology and methods available to use them correctly. A solution to this dilemma is to create systems and software where privacy by design is pre-installed and standard, and whereby the user is informed immediately the privacy protection system is compromised. One example of this is the TOR browser bundle, a software package small enough to be loaded onto a portable memory stick. When it is used, the web browser always attempts to open an encrypted connection and messages cannot be sent unless TOR has opened an anonymous communication path to the Internet. Sida (the Swedish International Development Cooperation Agency) is giving financial support to informing Internet activists in many countries about TOR and its capabilities.

If privacy by design and automatic warnings were standard in software then users would be able to benefit from security methods without needing to understand them fully. Companies could for example impose time limits for data storage to ensure automatic erasure after a predetermined time unless the customer prevents this, or to encrypt all communication with the customer. Encryption is an important complement to anonymity – it is meaningless to hide the origin of a message or the address of the receiver if information is sent in clear text. High-quality encryption is not necessarily expensive or difficult to use and could be implemented to a far greater extent than is currently the case.

### Political and economic driving forces

Legal limits on what information may be collected and stored on the Internet are often based on a simple observation: when we are offered inexpensive goods or services we are likely to disclose our identity and our personal preferences, even if in opinion surveys we say we would prefer to remain anonymous. This information has a commercial value since it allows customer profiling and personalised marketing. This increases the possibility for individual pricing – someone who buys Gucci accessories may be prepared to pay more for everyday items like books and groceries. On the other hand, private information voluntarily shared publicly may be to the consumers' advantage. The Swedish national newspaper Svenska Dagbladet recently published a mortgage interest rate map where anyone could reveal private information on their mortgage interest rate. Thousands responded and the wide differences that were revealed resulted in

pressure on banks to be more transparent with their interest rates. In this type of situation it is in the company's interest to keep the customers' contracts secret, since ignorance weakens each customer's negotiating position. The aggregated and continuously updated mortgage rate map based on the newspaper's readership, which voluntarily disclosed information, is not possible in a traditional print newspaper. Disclosure of personal information often results in offers of cheaper goods and services in return – it is doubtful if the circa 400 million Google mail users are prepared to give up their free but advertising-financed service and pay for their e-mail, even if they made a conscious and informed decision.

Studies published by Ghose and Rajan (2006) have shown that regulations to strengthen integrity and security also risk reducing competition and productivity in the economy, not least because this disadvantages small and medium-sized companies. Such effects also explain why large companies sometimes lobby regulators with proposals and demands for new or modified regulations. Behind the rhetoric often lies a desire to obtain a market advantage over smaller and weaker competitors. The price for poorly thought-through regulation can be high in the form of delayed growth and innovation. This applies especially to the unpredictable IT industry.

At the interface between civil society and the state the right to privacy can be seen as double-edged. Investigative journalists have revealed how they use social media under false identities to cultivate contacts with politicians, and regard this as a natural part of their work to investigate the holders of power. However, a journalist who relies on a shield of anonymity may be tempted to cross legal and moral boundaries and encroach on the private life of others, as occurred in the British News of the World newspaper scandal which was exposed in 2011. When this happens one can question if anonymity on the Internet helps or hinders democracy.

The sanctity of our private life is sometimes used as an excuse to shield those in power from critical investigation. In 2007 the regime in Kazakhstan closed down the oppositional websites which had published revealing documents about the authoritarian President Nazarbayev. When EU Commissioner Viviane Reding suggested a "right to be forgotten" she was sharply criticised by among others Reporters Without Borders, who claimed that the proposal posed a threat to freedom of speech. Additionally, such erasure regulations would be difficult to impose in practice. Future solutions such as automatic erasure after a certain time may help, but because archived information in company systems may have a lifetime of decades impetuous regulation may incur enormous costs.

States not only create laws but also collect information, and are extending their technical and legal powers to monitor Internet traffic the world over. Repressive states such as Russia and China use such data to subdue critical opposition. The debater Evgeny Morozov has controversially written about "why the KGB wants you to join Facebook". In the wake of the Arab Spring, many would like to monitor who does what on the Internet – and torture undesirable elements, as in Bahrain, or imprison them, as occurred in Egypt even after the fall of the Mubarak regime.

Reding's proposal was part of a review of the EU's data protection directive, where the European Commission and European Parliament have made different proposals. In the USA there are also proposals for harder regulation. The Federal Trade Commission has imposed stiff fines on companies such as Facebook which were careless in their handling of customer information. In February 2012 President Obama presented a Consumer Bill of Rights containing new regulations on the way companies handle personal data. This trend towards new regulation on both sides of the Atlantic may have important consequences far beyond the IT world. In the 1990s both the USA and the EU introduced different regulations to protect personal information. This might have initiated a trade war if agreement on a compromise had not been reached. As negotiations on a transatlantic free trade agreement are now maturing it is strategically important that regulations on protection of personal information do not hamper this. A successful free trade agreement is expected to lead to a 20 per cent increase in transatlantic trade.

The international nature of the IT market means that companies in small, export-dependent countries like Sweden may face a dilemma: products which are used for crime prevention in one country may be used for repression in another. The technology paradigm "privacy by design" does not offer a simple solution since the protection of privacy involves not only technical but also regulatory and organisational factors. Moreover, regulations which allow a state legitimately to gather data in a well-functioning democracy can still be misused and used to oppress citizens in countries with less well-developed democratic values.

That regulations are needed to ensure that companies respect their users' privacy is perhaps no longer self-evident. Microsoft now markets the e-mail service outlook.com by attacking Google which uses Gmail content for direct marketing. With the slogan "Think Google respects your privacy? Think again", Microsoft is attempting to reach the increasing numbers of users who wish to protect their privacy. Microsoft is not alone – those who are concerned about questions of integrity represent an increasingly powerful customer

group. Google for instance now informs Gmail users if there are indications that a state organisation has attempted to hack into their accounts. If sufficient numbers of customers start to vote with their feet this will encourage companies to change their policies – and this is likely to bring about change much faster than new regulation.

### Outlook for the future

The possibilities for digital communication and data transfer are in no way exhausted, and the pace of development shows no sign of slowing. New technologies for remote control of electricity consumption in our houses, remote monitoring of a heart patient's pulse or biometric methods for identification open up new opportunities for use and misuse. It is an unfortunate problem that consumers, companies and states are often blind to the negative sides of digital technology.

The question of who really owns information about us, and what it may be used for, is unfortunately not raised often enough. Even though it is not an easy question to answer it is a good point to start from. Concomitantly the user must also be aware of possible consequences, and not least the limits of regulation which often lags far behind technological development. Changing one's supplier in many cases produces more rapid results than new laws – but it also demands that one is aware of the possibilities of new technology. New software design principles, whereby privacy protection is pre-installed, demand less understanding from the user. Impetuous regulation of privacy on the Internet may do more damage than good, and may unintentionally favour larger companies over their smaller competitors.

Repressive states will always attempt to monitor and suppress critical opposition. It is a fact that new technology gives them new opportunities to do this. Simultaneously we can see from events in North Africa that technology can also be used to resist oppression. A race is in the making and it may be that new technology will help the revolutionaries more than the sitting powers. Many authoritarian states have studied and learnt from events in Egypt, Tunisia and Libya and are monitoring the Internet carefully. This agenda makes greater demands on countries such as Sweden which wish to enhance and spread democracy throughout the world. Foreign policy in the information society demands an understanding of what technology can – and cannot – achieve.

## Further reading

Brynielsson, Joel; Johansson, Fredrik; Jändel, Magnus (2013) *Privacy-preserving Data Mining.* FOI-R--3633-SE. Available from www.foi.se.

Franke, Ulrik (2012) *Disconnecting digital networks: a moral appraisal*, International Review of Information Ethics, Vol. 18, pp. 23–29.

Ghose, Anindya; Rajan, Uday (2006) *The Economic Impact of Regulatory Information Disclosure on Information Security Investments, Competition, and Social Welfare, in Fifth Workshop on the Economics of Information Security.*

GPS jammer connected to the cigarette lighter socket in cars.
(Photo: Peter Johansson, FOI)

# The Wireless Society – A Colossus with Feet of Clay?

Peter Stenumgaard

*The number of mobile subscriptions in the world passed 6 billion in 2012. In 2010, Sweden had more mobile than fixed broadband subscriptions. The use of wireless technology is also increasing rapidly in critical societal functions such as energy production, transport, logistics, banking and financial systems, and industrial and security applications – this despite the fact that the civilian wireless technology is very sensitive to interference signals. Hitherto only military actors have been able to utilise this sensitivity effectively, but this ability is spreading to civilian actors, thanks to sophisticated jamming equipment which is now sold openly and inexpensively via the Internet. Already today, jammers are being used to knock out vital communications, positioning and alarm systems in connection with rioting and criminal activity.*

## Rapidly increasing use of wireless communications

The use of wireless technology has exploded in recent decades and has led to most individuals today using such technology in some form. Today there are almost as many mobile subscriptions as there are people on the earth. However, not only is the use of wireless technologies increasing among individuals; it is also a general trend in society. Communication between different systems is usually called machine-to-machine (M2M) and may include communication between different sensors to computer systems for monitoring and control. The M2M market is growing very fast, and the wireless part of M2M grew by 37 per cent in 2011 and, according to forecasts, will continue to grow in the coming years. We can see rapidly increasing use of wireless technologies in critical societal functions such as energy production, transport, logistics, banking and financial systems, and industrial and security applications. Within industry, wireless technologies are increasingly used for monitoring and real-time control of processes and machines. Wireless technology is also common in various types of alarm systems, such as burglar alarms, shoplifting alarms and alarm systems for cash in transit (CIT). In both aviation and maritime applications, wireless technologies are used for voice communications, identification, navigation and surveillance.

## The need for wireless technology

For some activities, wireless technology is a necessity. In military operations, reliable wireless technology is a prerequisite for success. Similarly, wireless technology is often a key factor in the work of

police, rescue and medical personnel. There are several examples of the very serious consequences of radio communications being disturbed in such settings. As an example, this issue came to the forefront in April 2008, when two firefighters in Cincinnati died in a blaze on Squirrel's Nest Lane. A review of the radio calls made during the fire showed that the firefighters repeatedly made mayday calls which were never transmitted. The International Association of Fire Chiefs has released an interim report concerning possible communications problems involving digital two-way portable radios in close proximity to common fire-ground noise.

Another example of the importance of robust wireless communications comes from the terrorist attack in Norway on 22 July 2011. According to media reports, the new digital radio system for first responders did not have sufficient coverage at Utøya, prompting the district police to use the older non-encrypted analog system. The elite Delta unit, dispatched to tackle the gunman, and paramedics had switched to a new, secure digital network. The consequence was that the operation was delayed since police commanders had to contact different units via email and even fax, as the mobile network was down. It was down due to overload because too many people were trying to call from their mobile phones. During the Gothenburg riots in Sweden in 2001, the demonstrators caused interference in the police radio system. This interference contributed to the chaotic situation that arose, and led to prosecution for gross sabotage.

Another important example of vital wireless technology is the Global Positioning System (GPS) which is used for both navigation and positioning of personnel and units, as well as sending an accurate time signal to telecommunications networks. One example is using the GPS signal to ensure that the world's stock markets have common time so that no operator using automatic electronic trading (robot trading) can take advantage of the time signal differing between two stock markets. GPS receivers, however, are very easy to disturb because the power in the received satellite signal is very low. This, combined with the rapidly increasing dependence on GPS in critical security applications, opens up great vulnerability to intentional interference transmission.

### Why is wireless technology vulnerable to interference?

All wireless technologies are designed to intercept the radio signals in the air. The problem with this is that other signals that are in the air can enter the receiver, which then becomes disturbed. As everyday consumers we do not stop using cell phones even if a call is often broken when we are, for instance, travelling by train. Nor do we stop using wireless Internet, even though sometimes we do

not make contact or the connection is slow at times. However, if we had a car that had the same reliability as wireless consumer devices, most of us would try to sell the car as soon as possible. When it comes to wireless technology, we have accepted that reliability and availability vary. This acceptance of disturbances is taken into account in prioritisation of technical features in the development of wireless technology for everyday consumers. High immunity to noise always comes at the expense of capacity in the form of a reduced data transmission rate (a slower connection) or fewer users being able to use a system simultaneously. In civilian wireless systems capacity is always prioritised before immunity to interference. This is due to commercial reasons. In military wireless communications, as well as space and some industrial applications, immunity against interference is prioritised when it is important to always maintain contact: interference problems can cause both material and personnel losses.

### Radio interference

Problems with radio interference caused by unintended interference signals from electronic systems have been known since radio's infancy and came into focus when radio broadcasting started almost 100 years ago. The realisation that the electrical systems in homes could disrupt the radio signal being received led to the development of standardised values for maximum emitted radio interference from electrical equipment.

Radio interference can have different origins. The concept of "man-made noise" is usually used for general environmental noise generated in urban areas and close to industries. What the different types of noise have in common is that this interference is generated by various activities and processes involving electronic equipment.

Locally generated interference signals come from the various electronic systems in the vicinity of a receiver. Equipment that generates high levels of radio interference includes, for example, personal computers, charging equipment for battery-powered products, microwave ovens and low-energy lamps. Locally generated noise is a growing problem that is increasing with the quantity of electronic equipment used in both private and commercial activities. More or less serious incidents caused by accidental disturbances are reported regularly. A recent Swedish example is from 2011, when a large electronic billboard disrupted the flight radio during take-off and landing at Trollhättan airport. The third group of interference signals is from intentional jamming by transmitters in order to hinder or completely block wireless communication. For example, jammers were installed in the Sistine Chapel in Rome to prevent communication between the cardinals and the outside world in connection with the election of a new pope.

### Military capability is spreading to civilian actors

In military operations, it has always been a well-known fact that effective wireless communication is a prerequisite for command and control. For this reason, radio interference is an established and well-known method of effectively reducing an opponent's ability to lead his units. Historically, tactical jamming of the radio has been, with few exceptions, a purely military capability. Today, this ability has started to spread among illegal actors in society, which means a rapidly growing threat to critical wireless communications, for example, police, rescue services, wireless alarm and surveillance systems. The ability is spreading as jamming equipment is now sold at low cost via the Internet (see illustration). The fact that the use and possession of jammers is prohibited in many countries has not stopped the market for these growing rapidly in recent years. A player who wants to use jamming can already for a few hundred dollars buy a jamming device adapted to any existing civilian wireless system. So far, the ability to use these jammers has been limited to single events during riots and theft. However, evidence suggests that the ability is evolving towards continued increased understanding of how this technology can be used, well synchronised with other activities at more advanced operations and more complex targets.

### Examples of illegal jamming events

Disturbance of police radio systems began to happen in the early 2000s in connection with demonstrations and riots. Examples of this being highlighted in the media occurred at the World Bank meeting in Prague in 2000, at the EU summit in 2001 (the Gothenburg riots) and at the riots in Sydney (Cronulla and Brighton le Sands) in 2005. At these events either pure jamming and/or transmission of false calls were used to cause confusion in the police operations.

Swedish and international media regularly report jamming being used in connection with theft and burglary. A common target is alarm systems that use wireless technology. Examples of alarm systems subjected to jamming are shoplifting alarms and burglar alarms, home alarms and assault alarms for CIT and limousines. Jamming of GPS receivers has been reported for a variety of GPS applications. This includes, for example, GPS receivers used to track valuable cargo or to register routes for various commercial vehicles. Near North Korea's borders numerous cases of jamming against airborne GPS receivers have been reported. Furthermore, jammers are also used to block wireless locks in cars so that the car is not locked when the owner presses his wireless key. This technique is typically used in large car parks , and means that the owner does not notice that the car is unlocked. When the owner has left the car, it is emptied of valuables.

### Consequences from an international perspective

Within Europe technology-oriented systems for protection against terrorists and organised crime are developing rapidly. These systems often put great trust in wireless technology to connect different sensors and positioning and monitoring systems. As more countries are increasing their use of wireless technology in critical applications, their vulnerability to intentional jamming is seriously increased. There are European examples of protesters jamming police radio systems and criminals using jamming in connection with criminal activity. In the EU, most countries, like Sweden, have chosen the TETRA standard for radio communications for police, rescue services and ambulances. TETRA-based systems are built to be secure against eavesdropping, but they are actually just as susceptible to radio interference as older radio systems. This vulnerability is particularly problematic as the ability to disrupt transmissions is also increasing among non-military actors. The growing presence of jammers in itself increases the risk of pure accidents if the jammers accidentally knock out vital systems. One example is from Newark Airport in New Jersey in 2009, where several of the airport's GPS receivers were being knocked out at regular intervals. After a long investigation, it turned out that it was a passing lorry that had disrupted the GPS receivers. The lorry driver had installed a GPS jammer to jam the GPS receiver that the employer used to log drivers' routes.

There are, as we have seen above, several examples of the loss of radio communications in emergency operations leading to death and delays. The increasing use of GPS in critical societal systems and military weapons amounts to a global vulnerability that can cause very serious problems if an attacker chooses to combine its operations with jamming.

### Consequences from a Swedish perspective

Sweden is among the countries in the world that have been quick to introduce wireless technology in many applications that affect civil security and crisis management. This is natural since Sweden has had a leading role in telecommunications for a long time and was early to use wireless technology throughout society. The downside is that the vulnerability of wireless technologies is spreading more rapidly in Sweden than in other countries where the use of wireless technology has not yet penetrated as broadly. As a result, there are now plenty of Swedish examples of criminals using jammers against alarm systems, car locks and stores' anti-theft systems. The fact that non-military actors have started to acquire the ability to use jamming is also a growing threat to the ability to maintain critical communications during operations of all kinds. The Gothenburg riots clearly demonstrated that disruption of the police radio communications can seriously hamper the effort and contribute to a

situation becoming chaotic and difficult to control. GPS is used to a great extent in Sweden, both for positioning and for signalling the time to telecommunications networks.

A continued increase in the use of interference-sensitive wireless technology in critical societal functions dramatically increases vulnerability to both accidental and intentional interference. As the ability to use jamming is increasing among civilian actors, this is important to consider over the next few years in all situations where wireless technologies are being considered for critical societal functions. Any naive confidence in wireless technologies leads to a very vulnerable society.


The Volga-Urals region and the North Caucasus are areas predominantly inhabited by Muslims. (FOI/Natural Earth 2013)

# Russia and Islam – A Political Balancing Act

Johan Norberg

*Russia's great power ambitions can partly explain its Middle East policy, which mainly benefits Shiite actors such as Iran and the Assad regime in Syria. Russia's political leadership is probably aware that such a Shia-oriented foreign policy is alienating the world's Sunni Muslims, the majority in Islam. It also knows that this can affect Muslims in Russia and the former Soviet Union, where Islam is not yet a political force as it is in the Middle East after the Arab Spring. There is an increasing emphasis in Russia on an ethnically-based patriotism as a unifying political idea. This may in the long run increasingly alienate the country's 15 million Muslims, which in turn may exacerbate separatism and increase the risk of terrorism. Russia's relations with Islam thus affect both the country's foreign and its domestic policy.*

Russia's support for primarily Shiite actors such as Iran and the Assad regime in Syria, whose members mainly come from the Shia minority Alawites, means that Russian policy is increasingly seen to have taken sides in Islam's tension between Sunnis and Shiites. Russia's Muslim minority (mostly Sunnis) of about 15 million people, over 10 per cent of the population, have since 1991 been increasingly affected by currents within the umma, the global Muslim community.

Russia's political leadership is performing a balancing act. On one hand, there is a tradition whereby the Russian state recognises and supports some organisations as representatives of the forms of Islam that traditionally exist Russia. These types of mostly moderate Islam, closely linked to various ethnic groups, have through such organisations become allied with the Russian state and are here called state-sponsored Islam.

After the fall of the Soviet Union, on the other hand, many Muslims are increasingly questioning state-sponsored Islam, and this is undermining the state's influence. Russia's political leadership has more and more had to cope with new influences from global Islam such as fundamentalism, extremism and violent radicalism, here simplistically called Islamism. There is concern that Islamism can be pitted against state-sponsored Islam and nourish both terrorism and separatism. How is the Russian political leadership's Middle East policy linked to the way in which Islam is developing in Russia?

### Russia in the Middle East – ambition, fear and credibility

Great power ambitions, fear of radical Islam and a desire to be a credible ally are possible driving forces in Russia's Middle East policy. Its great power aspirations can be seen in the long-standing support for Iran, which gives Russia some influence in the region as well as a role in the international efforts to address Iran's nuclear energy programmes. Support for the Assad regime in Syria gives Russia a central role in the international effort to resolve the conflict there politically, which can be presented to Russians as increased global influence. The notion that Russia is a great power is uncontroversial in Russian domestic politics and useful to placate public opinion.

Another driving force may be that Russia's political leadership is concerned about the growing influence of fundamentalist Islam after the Arab Spring and how it can affect both the Middle East and Muslims, for example, in the former Soviet Union. A third explanation could be that the Russian political leadership wants to strengthen its credentials as the main ally in the Collective Security Treaty Organization (CSTO), a military alliance between Russia, Kazakhstan, Kyrgyzstan, Tajikistan, Armenia and Belarus. If Russia's allies see that it is letting the Assad regime, a close partner for decades, down, Russia's credibility would suffer.

### Moscow has become "Islam's enemy number one"

Russia's support for Iran and Syria creates friction with Sunni countries such as Saudi Arabia, which plays an important role in the Middle East and within Sunni Islam. In February 2012, Saudi King Abdullah criticised Russia's and China's veto in the UN Security Council against external intervention in the Syrian conflict. In the ensuing debate in the (Sunni) Arab press, there were calls for both an Arab boycott of Russian and Chinese goods and death threats against Russians and Chinese in Syria. Russia's relations with Saudi Arabia and the Arab League – from which Syria was expelled in 2011 – deteriorated.

The criticism of Russia in the Saudi press revolved around a few themes. The first was that Russia, by joining in the Iranian-led Shiite camp, has distanced itself from the Sunni Muslim world. An editorial in the influential Saudi daily Al-Sharq Al-Awsat in March 2012 named the Russian Foreign Minister, Sergei Lavrov, "Mullah Lavrov". In October 2012 Yusuf al-Qaradawi, an Egyptian television preacher, reportedly with some 60 million viewers and close links to the Egyptian Muslim Brotherhood, called Russia "Islam's enemy number one". His views may influence Sunnis, not only in the Middle East. They may also suggest how Russia is viewed by the Egyptian Muslim Brotherhood, which controls the region's most populous country. Russia is also criticised for ignoring Syria's Sunni

majority and the Moscow-backed regime in Chechnya is compared to the repressive minority rule of the Syrian Alawites. A third theme is that the Russian policy is strengthening the sectarian conflict in the Middle East, which in turn could affect Russia itself in the form of increased ethnic and religious conflicts or insurgency movements like the Arab Spring.

### Consequences for Russia

Sunni Muslim anti-Russian rhetoric in the Middle East could eventually increase Russia's problems with separatism and terrorism. Anti-Russian sentiment in the umma could radicalise Muslims in Russia who feel alienated from Russian society and state-sponsored Islam. It could also influence migrant workers from former Soviet republics who are mistreated in Russia, and increase the risk of Russia becoming the target of global Islamist terrorism.

Islam has long been a part of Russian society, especially in the North Caucasus and the Volga-Urals region. Today, Muslims live all over the Russian Federation. In addition, there are migrant workers, mainly from the former Soviet republics, many of whom reside in Russia illegally. No one knows how many they are, but figures of up to a few million are cited in the Russian press.

The Russian political leadership does not seem to have a problem with Islam as such. The problem is rather when religion becomes a political force, either as it has become in the Middle East after the Arab Spring, or as a result of radicalisation. The Russian researcher and Islam expert Alexei Malashenko notes that Russian politicians and experts believe that Russia's Muslims are gradually becoming radicalised. Mainly young people are becoming disillusioned with state-sponsored Islam and attracted to Islamism. Islamism is often in conflict with state-sponsored Islam in the North Caucasus, where it has had a greater impact than in the rest of Russia.

Islamism could worsen two already substantial problems for Russia. The first is its territorial integrity. Since 1994, despite two wars and major military operations, the Russian central government has had increasing difficulty controlling the North Caucasus. The second is terrorism, which many in Russia believe is related to the first. Since 1996, 26 terrorist attacks have reportedly killed more than 600 and injured more than 900 people in Moscow alone.

The Russian political leadership seems well aware of the risks. Different doctrine documents reflect concerns about trends of increasing extremism. The National Security Strategy 2020 says, inter alia, that a "development of nationalist sentiment, xenophobia, separatism and violent extremism, which among other things can make use of slogans

of religious radicalism" is having a negative impact on Russia's ability to protect its national interests. Russia's Military Doctrine from 2010 describes the basic external military dangers for Russia. Among these are "... a growing separatism and violent (religious) extremism in some parts of the world". The Russian political leadership is probably concerned that upheavals near Russia, such as those in Georgia in 2003, Ukraine in 2004 and Kyrgyzstan in 2005 and 2010, were not the last.

The Russian military also follows developments closely. The Chief of the General Staff, Valery Gerasimov, said in February 2013 that the handling of the Arab Spring reflects how future conflicts will involve not only the use of military means but also political, economic, humanitarian, and information resources. In the autumn of 2011, the Russian Armed Forces conducted their annual strategic exercise in Central Asia, together with Russia's allies in the CSTO. The newspaper Rossiiskaia Gazeta, close to the Russian government, quoted former Chief of the General Staff Nikolai Makarov as saying that events in the Middle East indicated that Russia must be able to intervene against unforeseen events in Central Asia. The Collective Operational Reaction Forces that Russia and its allies in the CSTO have set up consist mainly of mobile airborne units that can be rapidly deployed to address a quickly emerging crisis, but would have limited endurance without reinforcements, especially against another regular military force.

### Challenges in the North Caucasus, the Volga-Urals and Moscow

The relation to Islam influences Russian policy in three important regions. The first is the North Caucasus. The conflict in Chechnya, initially a struggle for greater autonomy, power and resources, gradually acquired a religious character. For nearly 20 years, the Russian central government has tried approaches ranging from suppressing the area with military force to designing regional support measures that in practice buy the loyalty of local elites. Yet it is hard to see that the Russian central government is in control. There are fears that a similar development, an independence quest turning into armed struggle with religious overtones, could occur elsewhere. Without specifying the enemy, President Putin said in an interview book in 2000 that Chechnya is a beachhead for further attacks deeper into Russia, including the Volga-Urals region, which is the second area.

The Volga-Urals region includes the relatively developed and resource-rich republics of Tatarstan and Bashkortostan, with nearly 8 million inhabitants between them, most of them Muslims. The area is located centrally in the Russian Federation and roads, railways

and other infrastructure that connects western Russia with Siberia and the Far East pass through it. Weakened central control here could make it difficult to hold the vast country, spanning nine time zones from west to east, together. The Russian political leadership is probably worried when politicians in the Volga-Urals talk about independence. Signs of growing tension with the federal government in Moscow can be seen in symbolic issues. In Tatarstan many were irritated when the central government in Moscow wanted to stop compulsory instruction in schools in the local language alongside Russian. In late 2012, the newspaper Izvestiia reported on ideas that a Russian constituent republic's name should not include references to dominant population of the republic. Reportedly, many in Tatarstan were furious. The Tatars' World Congress, an organisation allegedly close to the republic's intellectual and political elite, even suggested in December 2012 that Tatarstan should seek observer status in the UN.

In the Volga-Urals region, violence seems to be escalating both in the conflict between state-sponsored Islam and Islamism and in connection with possible separatism. In the summer of 2012, Tatarstan's Deputy Chief Mufti was shot dead in the republic's capital, Kazan. The chief Mufti was injured by a car bomb. Radical Muslims were identified as the culprits, although press reports claimed that it could also be a dispute about money. In December, in the neighbouring republic Bashkortostan, the Russian Interior Ministry deployed its military units against what the ministry called "nationalist band formations". The central government in Moscow seems to think that the challenge is the same as in the North Caucasus – Islamism as the basis for separatism. Countermeasures include a preparedness to use violence, regional funding and installing regional leaders who are loyal to the central government. There should, however, be few Islamists in the Volga-Ural region.

The third area is Moscow, with one of the largest Muslim minorities of any European city. Of some 13 million inhabitants, up to some 2.5 million were Muslim in 2010. Many of them are probably secular and do not constitute a coherent political force. There is nevertheless a possibility of friction with Russian society. The five officially recognised mosques are too few, given the sizeable labour immigration, especially from Muslim countries in Central Asia, and the fact that many of these immigrants increasingly follow Islamic rules of life. The lack of public mosques could lead to many Muslims seeking out informal mosques, which more often harbour more radical forms of Islam. Russian police often raid informal mosques, although with few arrests as a result. The building of new mosques often meets with local protests, as it did in the Moscow suburb of Mitino. Protests occur elsewhere too, for example in Stavropol in

southern Russia, where tensions between Muslims and Orthodox Christians are strong.

### What is the place of Muslims in a more patriotic Russia?

The Russian political leadership has for many years pushed increasingly patriotic ideas in order to strengthen its own legitimacy. There is, however, a risk that such ideas will strengthen Islamism or separatism in multinational Russia. According to Gudrun Persson, a Swedish specialist on Russian politics, this Russian patriotism has three components: a strong central government, the perception of strong armed forces and a strong Russian Orthodox Church. Russian ethnicity, the Russian language and Russian culture play a central role. But how is it perceived by Russian citizens who may feel that they are not embraced by these patriotic ideas, such as Muslims, for example in the Volga-Urals and North Caucasus? How will it affect their loyalty to the Russian state? If the Russian political leadership pushes patriotism too far it could alienate more minorities, which in turn may increase the appeal of Islamism and separatism.

There are several areas of conflict between Islam and Russia's current policies, both domestically and abroad. So far, no spark has taken hold. Few of Russia's millions of Muslims have become radicalised. Islamism, however, could increasingly become an option for those who want to empower themselves and take control over their lives. The Russian political leadership's long-term ability to manage the inherent diversity in its society is important for keeping the country together. The last decade's upheavals in former Soviet republics and the Arab Spring have probably accentuated Russia's struggle with Islamism and separatism. Russia's national and religious diversity limits how far one can push an ethnically marked patriotic mobilisation. If the Russian political leadership ignores this, the consequences could be dire. Russia's relations with Islam affect the country's stability and long-term development and are thus of great importance to the world, not least to Russia's neighbours and trading partners.

## FURTHER READING

Hedenskog, Jacob (2011) "Russian Worries over Terrorist Threats to the 2014 Winter Olympics" in Hellström, Jerker et. al. (eds.) *Strategic Outlook 2011*, pp. 21–28. FOI-R--3210--SE.

Hedenskog, Jakob (forthcoming 2013) "The Terrorist Threat Against Sochi-2014", in Bo Petersson and Karina Vamling (eds), *The Sochi Predicament: Contexts, Characteristics and Challenges of the Olympic Winter Games in 2014*, Cambridge Scholars Publishing.

Norberg, Johan (2013) *How Some of Moscow's Middle East Interests Could Create Problems for Russia*, FOI RUFS Briefing No. 17, January.

Norberg, Johan (2012) *An Attack on the Iranian Nuclear Programme – Some Possible Russian Considerations*, FOI, RUFS Briefing No. 13, June.

# Chemical and Biological Weapons – Soon Available to Anyone?

Elisabet Frithz and Per Lind

*The globalisation of industrial production is greatly influencing the structure of the chemical and biotechnology industries. In the last decade countries such as China and India have emerged as leading global producers and exporters of chemicals. What consequences will this have on the ability to control the international trade in hazardous chemicals? What effect will it have on the West's ability to prevent the proliferation of potentially dangerous products and know-how, when research and development of biotechnology is also increasingly globalised? The international community faces new challenges in its efforts to enforce non-proliferation and prevent the growing threat from biological and chemical weapons.*

Western Europe and the US long dominated the chemical industry and the manufacture of process equipment. When the outside world inspected the Iraqi facilities for proof of chemical weapons in the aftermath of the 1980-88 Iran/Iraq war, it was found that some of the precursor chemicals and materials used for its Chemical Warfare programme had been imported from the West. To prevent future recurrences of such proliferation Australia initiated the forming of the Australia Group (AG) with the aim of harmonising national licensing measures and export controls. The group today comprises, among others, the USA, Canada, Australia and the member states of the EU. The aim of the AG is to control specific processing equipment and material that might be used for manufacturing chemical or biological weapons and prevent it from being exported to states or actors who might misuse this technology.

However, since the AG was set up in 1985, the global spread of processing equipment, chemicals and biological products has increased. It is mostly countries outside the AG, among them China and India, that have emerged as new suppliers. It can be worth mentioning that out of around 5,400 chemical production sites worldwide, which are obliged to declare their production according to the 1993 Chemical Weapons Convention (CWC) and therefore are inspected by the OPCW (the Organisation for the Prohibition of Chemical Weapons), around 1,500 are situated in China, and around 600 in India.

However, globalisation is not only affecting the chemical industry. Many Asian countries have identified biotechnology as a key factor in their economic growth. For example, China has one of the most important research institutes for DNA sequencing. Statistics show that countries in Asia progressively climb towards the top when it comes to scientific publications and market shares within biotechnology.

These developments raise many questions concerning the effectiveness of export control and our ability to prevent the proliferation of what we call dual-use products, that is, products and material that have both civilian and military applications. The fact that big producers such as China, India and Russia are not members of the AG does not automatically imply that any state or group can procure sensitive equipment from these countries. However, there are challenges regarding the harmonisation of export control systems, mainly in respect of the implementation and observance of the laws. In other words, it is of the greatest importance that states draw up mechanisms to guarantee that legislation is followed in order to prevent smuggling and proliferation of this kind of products and material.

### What happens when research and development is globalised?

The production of chemicals has been relocating to low-wage countries for some time. In recent years, however, research and development has also more and more been relocated from the Western world, mainly to states in Asia. Currently, the power of innovation and technical advances still derives from the industrialised Western world, but given the prevailing trend a key concern is the future. Since countries in Asia are becoming more dominant in the production and development of chemicals, as well as the development of pharmaceuticals and biotechnology, there will be proliferation and globalisation within these areas. Knowledge dispersion in itself is not a problem; on the contrary, it is an important part of democratisation and economic growth. Problems might, however, arise when knowledge about the effects of new chemical and biological substances on the human body spreads to states and organisations whose aims and intentions are not always known to the rest of the world.

Yet another problem is knowledge transfer of sensitive technology. This is usually put under the heading of intangible technology transfer (ITT) and deals with questions about the transfer of information and knowledge needed for using, developing or producing an export-controlled product. As the

manufacturing of production equipment as well as chemicals and biological substances is globalised, this question will, to an even greater extent, have a great impact since we can no longer rely on the control of the trade in dual-use products performed by the AG countries.

The question is who in the long run will get hold of this new knowledge that is evolving in countries that lack the transparency and the approach that characterise the democratic world. What will happen if a closed country uses new technology in order to develop new chemical or biological substances that can be used in conflicts – substances that, today, are not regulated or specified in lists of substances that have to be declared?

### The development of technology is accelerating: faster, simpler, cheaper

The pace of development within biotechnology is steadily increasing. Sophisticated experiments which only a few years back demanded substantial resources, in the form of equipment and time, can today be done in small laboratories and almost be described as routine work. An area that has attracted a great deal of attention during recent years is so-called synthetic biology, which could be described as advanced genetic engineering and balances on the border between science and technology. The potential for synthetic biology lies in the possibility of creating artificial genes that are put together like Lego bricks to create the desired biological system. One probable development is that many of these Lego bricks will be standardised and obtainable for purchase over the Internet. Critics claim that man, with this technique, has finally begun to "compete with God". Even if it today is relatively hard to synthesise for instance a virus, the developments that are going on, point towards the fact that the basics – DNA synthesis – are going to be cheaper, faster, more effective and thereby also more accessible on the world market. What is difficult and time-consuming today can most probably be made much simpler and faster in the future.

An interesting phenomenon that illustrates the proliferation and democratisation of current biotechnology is the so-called garage biology or do-it-yourself biology (DIY bio) movement. This movement involves individuals who engage in biology in their spare time, with or without academic background. Experience and various tips are exchanged over the Internet, in different groups. A Danish paper summarised the concept as "create your own DNA code, engage a company to synthesise the gene, test it in a bacterium and change the world". Various biotechnology companies have started to sell equipment and

reagents meant for synthetic biology. The target group is amateurs as well as professionals. Equipment, for instance centrifuges, is obtainable on eBay. As yet most of the DIY bio movement's followers are in the USA, but it is spreading over the world. Authorities in the USA have identified the movement as a potential security problem and have approached the movement in order to strengthen security awareness among those interested in DIY bio. From an American point of view, there is an opportunity to use the movement as a channel for communicating biosafety issues to the public.

### The industrialisation of biology

Industry is increasingly using biological approaches in production. Many leading analysts claim that we are facing a social transformation on par with the way in which information technology over the last few decades has changed the world. Developments within synthetic biology will probably stimulate this trend as it becomes possible to design microorganisms able to produce exactly the substances or molecules of interest. When industrial and financial interests adopt the technology, it means that a commercialisation not driven by the scientific community is taking place. One hot spot is bioproduction of fossil fuels, such as diesel and natural gas, as well as ethanol and butanol. Development has come a long way and pilot plants are now ready for use. Another example for the future is the way in which the extraction of rare earth elements (see chapter 13) could potentially be optimised using synthetic microorganisms. The mining industry, already today, uses bacteria for extracting, among other things, gold and copper.

The industrialisation of biology as a science is creating new risks. There is concern that the technology, when manufacturing in industrial scale becomes possible, will open up for mass production and consequently be used for creating new generations of weapons. An actor could, in the future, design synthetic microorganisms and produce substances similar to the classical chemical weapons, and perhaps also new toxic substances with new properties.

The use of modified bacteria for producing chemical substances is an example of how the classical sciences of chemistry and biology converge. This convergence will most likely continue and result in completely new ways of producing for example chemicals and many different types of materials. Such a development, with an increasingly active industry, will over time create a more complex situation where the control of sensitive technology will be even more difficult.

### Can tomorrow's technology and knowledge be monitored?

Chemical industry today, its production processes and its products, is monitored and controlled within the legal framework of the CWC. The question to be asked is how new production techniques fit in with this set of rules. If chemicals in the future are manufactured using biological methods, it can be argued that the production process should fall under the 1972 Biological and Toxin Weapons Convention (BTWC), which lacks the verification mechanism of the CWC. It can be argued that the product manufactured is the essential factor that should be declared, rather than the manufacturing process. If adding the risk of new types of toxic chemical substances being produced, which today do not have to be declared, a totally new field will emerge. Furthermore there is a risk that this field will fall in the crack between the two conventions. Sweden and other EU-members must as a consequence consider how a new potential industry can be accommodated within the regulations of the existing conventions. It is thus, not only the sciences that are converging, but also techniques and manufacturing methods, and all of this have to be considered when working within the contexts of the CWC and the BTWC.

It is also important to decide how to handle the proliferation of potentially sensitive information which might contribute to the development of biological and chemical weapons. A current example is the research on the avian flu virus. A group in the Netherlands was able to show that with only five mutations the virus could be transformed to be airborne and transmissible between mammals. Prior to publication, intense international discussions took place, involving among others the World Health Organization (WHO), the USA and the Dutch government, since there was a fear that this kind of knowledge could be misused. The debate, which also involved the research community, clearly showed that different actors' attitudes to knowledge proliferation differ significantly. Some claim knowledge is beneficial whereas others claim that research should be governed by rules and regulations, since it is impossible to predict how new knowledge might be used. The big issue, however, is whether knowledge and knowledge dispersion can be controlled in today's world. The Internet offers free access to knowledge, and in a global perspective students and scientist are more mobile than ever.

### What is Sweden doing?

What is Sweden doing to secure increased responsibility within education and research? What knowledge do we have that could

be used for antagonistic purposes? With whom do we share this knowledge?

The debate concerning the avian flu studies illustrates that the issue of dual-use research is becoming increasingly demanding to handle. The questions embrace many different sectors in society, with many actors, where national security issues are only one of several aspects. There is a great risk that the question of how to handle sensitive knowledge and research can get lost among the different authorities and ministries. In Sweden, FOI together with the Ministry for Foreign Affairs has highlighted the dual-use question within the research community as one part of the work with the BTWC. In order to get an overall grip on the problem, many authorities need to get engaged in this matter. The dual-use theme could be part of basic education at universities, for instance within biotechnology and chemistry, in order to increase awareness of these issues. As of today, there is no focused initiative on this issue, not even at the level of postgraduate studies.

Several countries have made far more progress in these matters, for instance, some countries have established national advisory boards where research projects are scrutinised from a dual-use perspective, at the same time as awareness and security considerations are far greater. One example is the visa vetting system in the UK, where applications from guest students or researchers are examined from the point of view of the research or education area chosen. In this way the authorities try to prevent sensitive technology from being taught to actors with possible connections to antagonistic groups.

### The threat remains

With the present developments within technology and knowledge proliferation, the map is going to be radically redrawn when it comes to who has access to sensitive knowledge, the capacity to develop new types of chemical and biological substances, and the capacity to produce such substances. There is a risk that, despite all good intentions, new biological and chemical weapons will be developed using completely new methods. From that point of view the threat of actors using biological and chemical weapons remains, despite all the work that has been done, among other things within the framework of the BTWC and the CWC.

## Further reading

Carlson, Robert (2010) *Biology is Technology*. Harvard University Press.

Center for Biosecurity of UPMC (2012) *The Industrialization of Biology and Its Impact on National Security*.

# The Role of Environmental Crime in Terrorism, Conflict and Criminality

Annica Waleij, Birgitta Liljedahl, Kristoffer Darin Mattsson and Louise Simonsson

*Second only to the trade in drugs and weapons, environmental crime is the largest illegal business in the world. It is global, organised and transnational, and it is increasing. Even so, only a small portion of all breaches to environmental legislation lead to prosecution and conviction. Countering the problem will require targeted actions in the judicial system, the security sector, industry, development aid and the research community, as well as improved coordination mechanisms.*

Environmental crime typically refers to breaches of environmental laws or environmental conventions. These regulatory mechanisms are in place to minimise and manage harm to the environment and human health. Unlike other types of crime, environmental crime mainly affects the environment and ecosystem services, the latter meaning the functions of ecosystems that benefit human beings. Transboundary environmental crime, particularly illegal trade in animals and animal parts such as elephant tusks, but also that in hazardous wastes, is estimated to be one of the most widespread types of crime in the world. The trade is global, organised, large-scale and transnational and is therefore attracting increased attention from actors such as the UN and the EU. The share of environmental crimes that are detected and solved is relatively low, and the profits can be substantial. According to statistics from the Swedish National Crime Prevention Council (Brå), only in a fraction of all environmental crime cases reported in Sweden can a person be prosecuted and convicted. In states with low legal certainty the magnitude of the problem is greater. Since environmental crime is rarely detected there are large gaps in our knowledge about this growing type of crime. According to Interpol the international trend is similar in the areas of wildlife crime, illegal logging and timber trade, illegal fishing and the illegal trade in chemicals or hazardous wastes. There are also emerging types of environmental crime, for instance carbon credit fraud and criminal activities in the water sector.

## Illegal trade in electronic and hazardous waste

Manufacturing of electronic equipment is one of the largest and fastest-growing sectors in the world and sales of electronic products are rapidly increasing. Consequently, the demand for the natural resources needed for their production, especially rare earth elements,

is also increasing (see chapter 13). Moreover, the waste (so called e-waste) that arises at the end of the product's life span is increasing at the same pace. As a result, more shipments of used electronic equipment are taking place to and between developing countries. Some of this activity can be linked to organised crime. In Operation Enigma, a major crackdown recently conducted by the police, customs, port authorities and environmental agencies at ports in seven European and African countries, illegal e-waste was discovered in one third of the cases. The secondary market for electronics is large in Africa and sometimes it is difficult to determine what constitutes waste or a used product. This grey zone is exploited by criminals.

Despite the fact that e-waste is classified as very harmful to human health, the global capacity to manage it in a way that is safe for the environment and health is limited. Manual disassembly and open burning of e-waste, so-called smash and burn, in order to separate out the metals for recycling, is common. The remaining waste is then deposited in an uncontrolled manner which, depending on its dispersion characteristics, constitutes a local or even regional threat to human health and the environment.

Transboundary movements of e-waste to developing countries are regulated by international conventions, including the Basel Convention and the OECD control system. Despite this, the export of e-waste to developing countries is of increasing concern as the illegal part of the trade, which is estimated as having an annual turnover of billions of dollars, is increasing. Shipment costs are often very low, while the value of the final product is high. This makes the illegal trade very lucrative, especially when low-wage labour in developing countries can be utilised.

There are many examples of trade in and dumping of hazardous waste. One of the more well-known examples is the dumping of hundreds of tons of chemical waste in Abidjan in Ivory Coast in 2006. The waste was shipped into Abidjan via the Panama-registered Probo Koala, owned by the multinational company Trafiguera, with its headquarters in the Netherlands. At least 16 people died and over 100,000 people sought medical treatment for vomiting, nosebleeds or breathing difficulties. Another example is the Italian Mafia's trade in unsorted municipal solid waste, which is indiscriminately dumped on land or at sea regardless of content.

### Wildlife crime and trade in natural resources

In addition to its negative environmental impact, the illegal trade in endangered animals and their parts – called wildlife crime – fuels conflicts, corruption and violence. In the Democratic Republic of Congo, Kenya and Chad, for instance, park rangers have been killed

by poachers hunting for elephant tusks, rhinoceros horns and leopard skins. The revenue from this illegal trade as well as the trade in live animals such as snakes, monkeys and big cats is used to finance militias, including the Janjaweed in Darfur. In Asia, a corresponding illegal trade in, for example, tiger skins and the endangered snow leopard takes place.

In parts of Asia, Africa and South America, it is estimated that over 80 per cent of all timber that is exported has been illegally handled in at least one part of the production chain. As illegal logging often occurs in forests with high biodiversity, and a large part of Europe's timber imports, including Sweden's, comes from these regions, Sweden and Europe are in fact contributing to a major adverse ecological footprint. Indonesia, Papua New Guinea and Cambodia are especially hard hit; but the problem is globally widespread and is increasing as more land is cleared for domestic agricultural purposes or to secure fertile land for foreign investors in what is called the land grab.

Another area affected by organised crime is fishing. Illegal fishing affects fish stocks as well as the means of livelihood through fishing, thereby fuelling other illegal activities, including piracy off the Horn of Africa. Although much of the illegal fishing is small-scale, the overall magnitude of the problem of overfishing is so significant that it is estimated that the world's commercially available fish stocks will be exhausted by 2048, depriving millions of people of their main source of protein.

The financial revenues from the illegal trade in animal products and natural resources are substantial and are constantly finding new markets through the Internet. Only a small portion of the profits from these businesses benefits the local population in the affected areas. In the worst case they drive conflict or finance terrorist activities. One such example is seen in Somalia, where the extensive amounts of charcoal that is illegally produced and exported to the Middle East have links to Al Shabab.

Corruption is a major part of the problem with environmental crime. For example, corruption is a key element in the chain whereby illegally logged timber is transported and shipped from the country of origin to other parts of the world. Corruption is widespread in the water sector as well, where it is estimated to raise the cost of water supply infrastructure, dam projects, canals and tunnels by up to 40 per cent. This is a particularly serious issue since the UN General Assembly has declared access to water and sanitation as a basic human right.

### Illegal logging and timber trade threatens climate adaptation efforts

The world's forests absorb carbon dioxide from the atmosphere and convert it into biomass which then stores the carbon until the woody biomass is destroyed. Thus, when timber is harvested, greenhouse gases which contribute to climate change are released. Illegal logging represents 50–90 per cent of the total volume of forestry in the major producing countries, while the corresponding figure is 15–30 per cent globally. The economic value of this activity, including the processing of the material, is estimated at a value of 30 to 100 billion US dollars, or 10–30 per cent of the global timber trade. Meanwhile, billions of dollars have been invested in REDD+ (Reducing emissions from deforestation and forest degradation), a UN mechanism that aims to reduce the problems of deforestation in developing countries and global climate change. For REDD+ to be successful, communities must benefit more from preserving their forests than from environmentally degrading activities, including illegal logging. Illegal international timber cartels therefore represent a significant risk for effective climate change mitigation while also jeopardising development and poverty reduction.

This illegal activity is increasing and is becoming more advanced as cartels become better organised, and combine traditional methods such as bribery with more modern methods such as data hacking to forge transport licences and other necessary approval documents. In recent years illegal logging has also included advanced methods to conceal the activity as well as related activities such as "timber laundering". Illegal timber transport however differs significantly from the smuggling of, for example, drugs in the sense that when it crosses borders the timber has been declared to be a "legal" product. Transnational timber crime is therefore a huge challenge for the judicial system, customs and law enforcement.

### The significance for Sweden and Europe

Sweden and the EU are affected both directly and indirectly by environmental crime. There are examples of Swedish computers and other electronic equipment from both the public sector and private individuals ending up in Ghana, Pakistan or China. For instance, computers from Stockholm County Council have inexplicably been found in Accra's slums. After criticism from the EU, Sweden has increased its border controls and during the first nine months of 2012 strikes on 80 Swedish consignments destined for foreign countries were carried out. Approximately half of the shipments contained obsolete electronics that could thus be prevented from leaving the country.

At the same time, waste is being imported into Sweden to secure enough waste volumes to fuel domestic waste recovery and incineration facilities. For instance, the metal company Boliden Mineral has tripled its capacity to recycle electronic waste at its Rönnskär facility and is now one of the world's largest recyclers of electronic waste. The quality and origin of the data on imported waste are, however, often difficult to check and it therefore cannot easily be ruled out that criminal activity has occurred somewhere in the chain.

Serious types of wildlife crime such as illegal hunting for wolves and eagles are increasing in Sweden and transboundary violations of wildlife protection occur all around Europe. In 2011, Europol alerted the law enforcement community that an Irish criminal network was active in several European countries, including Sweden, in search of the horns from the endangered rhinoceros. Rhinoceros horn is desired by traders and the horns can be worth up to EUR 200,000 each.

There are also the security implications of environmental crime. Sweden is present on the international arena through (for example) industry, development aid, and peace-support and security-building operations. As environmental crime escalates the connections to and impact on the trade in small arms, terrorism and conflicts increase as well. In practice, this means that both civilian and military operations, as well as other activities, in crisis and conflict areas are likely – unconsciously, directly or indirectly – to contribute to the complex environmental crime economy, and thus negatively impact on the conflict or problem to be solved. The role of corruption in the environmental crime chain is also paramount and creates a grey zone in which everything from locally employed workers to social functions and politicians may be indirectly link to the environmental crime economy. According to the World Wildlife Fund, crime syndicates have for instance used diplomatic mail for certain types of smuggling.

Through the amendments to the Lisbon Treaty and the jurisprudence of the European Court of Justice, the EU must push for greater efficiency and coordination in the field in order to meet the high ambitions of the Union to protect the environment and facilitate sustainable development. Among other things, stricter legislation governing the collection and handling of electronic waste is expected.

### What is being done and what can be done?

The UN Office on Drugs and Crime (UNODC) has argued that more research is needed to understand the relationships between transnational illegal markets, organised crime and conflict. This need

has also been emphasised by the police, Interpol, the United Nations Environment Programme and the EU. However, some effective tools are already operational. An area on the rise in both the civilian and the military sectors is environmental intelligence, which has evolved dramatically in recent decades. Its benefits are currently highlighted not only by the Swedish Armed Forces, which utilise it to generate data on corruption and environmental crime when planning for overseas operations, but also by NATO and the UN. Environmental intelligence provides early indications of the types and magnitudes of environmental crime in a region. Techniques used include satellite imagery, Geographic Information Systems (GIS) and dispersion modelling of air, soil and water. There is, however, a need to develop models to estimate the hidden costs of environmental crime, for instance the impact of an increased frequency of flooding in areas of illegal timber harvesting or the social and economic impact of losses of ecosystem services.

A number of laws and codes of conduct exist, although some of these are subject to strong criticism for their perceived ineffectiveness. In the EU the so-called WEEE (Waste Electrical and Electronic Equipment) directive on the efficient collection, treatment and recycling of electronic waste is one example. FLEGT (the European Commission's Forest Law Enforcement, Governance and Trade), which means that companies importing timber into the EU market must guarantee that the products were legally harvested, is another. Furthermore, as mentioned above, the UN system has the REDD mechanism. Industry has Corporate Social Responsibility (CSR) codes, which means a social responsibility for businesses that includes sustainability aspects, and the anti-corruption research is part of EU's Seventh Framework Programme. Finally, poverty reduction is a key component to promote livelihoods that will be an alternative to environmental crime.

The selected initiatives mentioned above are positive, but more action from a number of players and improved coordination are still required to counter the problem of environmental crime. There are still many gaps in our knowledge about the links between environmental crime, organised crime, terrorism and conflict. The research community must seek answers to the mechanisms behind these types of crimes and develop methods to detect and prevent environmental crimes. Industry as well as the security sector must ensure that they do not directly or indirectly contribute to transnational environmental crime and must provide intelligence that can prevent or detect environmental crime or ensure that the perpetrators can be prosecuted and convicted. The development of codes of conduct and best practices should continue, but stricter implementation of existing rules is also a way forward. Coordination

between and within different sectors of society should also include development assistance, which must play a fundamental role in the fight against environmental crime. Without alternative income opportunities for local actors in the environmental crime chain there is little chance of successfully combating environmental crime. The possibility of public-private partnerships with local businesses, for instance, to construct environmentally acceptable recycling facilities for electronic waste or encourage ecotourism in areas rich in wildlife, are two concrete proposals.

## Further reading


Waleij, Annica; Liljedahl, Birgitta; Darin Mattson, Kristoffer; Louise Simonsson (forthcoming 2013) *The Role of Environmental Intelligence in Countering Environmental Crime and Corruption.*

Liljedahl, Birgitta; Waleij, Annica; Sandström, Björn; Simonsson, Louise (2012) *Medical and Environmental Intelligence in Peace and Crises Management Operation*.
FOI-S--4174--SE.

Waleij, Annica; Liljedahl, Birgitta; Martinsson, Erik; Martinsson, Emil; Wikström, Per; Sandström, Björn ; Edlund, Christina; Rudén, Fanny; Berglind, Rune; Eriksson, Håkan; Simonsson, Louise (2011) *Environmental Health Threats 2010: Global Outlook.*
FOI-R--3300--SE.

# The Sea – Border and Trade Route

Sören Jägerhök, Rolf Ragnarsson and Björn Larsson

*Piracy, terrorism and organised crime all constitute threats to international trade and shipping. Unless the authorities and commercial players can improve their ability to identify and handle these threats, the economies of Sweden and the EU as well as global growth will suffer. Systems incorporating modern sensor technology, information sharing and autonomous alarm functionality to detect deviations from normal can improve security at sea and in port.*

The external border of the European Union is predominantly a sea border. The coastline of the Union is longer than either that of the Unites States or Russia. Almost 90 per cent of EU trade with the rest of the world is carried by ship, as is a significant share of freight within the Union. Sweden is engaged in considerable activities to protect international shipping involving naval and airborne assets as well as personnel, and operations are carried out far beyond Swedish territorial waters. As an example, in 2013 both the Swedish Armed Forces and the Swedish Coast Guard are participating in the EU anti-piracy mission off the coast of Somalia.

The global importance of the sea as a trade route and the great monetary value of goods shipped make shipping a target of interest to organised crime and terrorists. Natural resources at sea such as fish and energy, and facilities for the extraction of electric power from wind and waves, are also relevant in this context. Refugees as well as traffickers and smugglers move across the sea due to differing political and economic conditions on the different sides of the sea. At the same time, ongoing climate change is creating new conditions for shipping in the Arctic waters, which in turn leads to new opportunities, risks and demands.

Shipping security is not only about surveillance of vessels at sea, but also includes the handling and protection of vessels, goods and passengers in ports and terminal facilities. Despite the importance of a secure and efficient system for sea transport, considerable deficiencies remain in the coordination of the security measures of the numerous different stakeholders involved.

### Crime at sea and in port

Smuggling in all its forms constitutes a serious problem for society. In addition to the damaging effects to society of the inflow of drugs, other types of smuggling such as the importing of imitation brand goods can cause great economic losses and occasionally health hazards. The current fast-growing trend towards the transport of large quantities of goods in closed, sealed containers makes large-scale smuggling operations more feasible as the sealed containers make the checking of actual contents against customs manifests more difficult. The metal container walls make the operation of capable inspection systems expensive.

Cavities in the interiors of trucks and train carriages can also contain contraband. Smugglers are known to fasten hidden containers on the hull below the waterline of merchant vessels; concealed divers then exchange these containers when the vessel is in port. Alternatively, larger vessels can throw parcels of goods overboard at pre-selected positions before entering port. Small fast boats are then deployed from land to collect the parcels. This method can be highly successful since current systems for sea surveillance often lack the ability to detect, track and identify such small surface vessels.

Another threat to the enormous value represented by goods being shipped is organised crime on land. Criminal organisations often have international ties and connections to seemingly legitimate parties that act as a façade. Calculations by the Dutch Professor Roos show that several per cent of all goods going through the port of Rotterdam during the 1990s were lost due to criminality. Despite improved routines and regulations after the terror attacks of 11 September 2001, large monetary losses still occur when goods are being transported through the ports of the EU. Detailed schedules for lorries loaded with valuable goods can also be leaked through corruption or negligence and make profitable thefts possible well outside the port area. Swedish and European competitiveness on the global arena is damaged by such losses. Profits realised from this type of theft and fraud can also enable criminal organisations to penetrate other sectors of society.

The nature of the piracy threat to sea transport varies depending on location. Around the Horn of Africa, the main risk is hijacking of an entire vessel and crew followed by demands for ransom. Piracy is also a risk along the west coast of Africa and in Southeast Asia, but in contrast to the situation on the Horn of Africa, there are no lawless ports where long-drawn-out

hostage negotiations can take place. Instead, night-time raids are common: the crews of vessels anchored outside a port are surprised while waiting for a berth.

According to Russian authorities, the Maltese-flagged vessel Arctic Star was hijacked in Swedish territorial waters while carrying what was declared to be solely timber between Finland and Algeria in July 2009. Three weeks later, the Russian Navy issued a statement that they had taken control of the ship close to the Cape Verde Islands. The real circumstances of the hijacking may never be stated officially, but the incident serves to demonstrate that the piracy problem is present closer to home than most of us think.

Terror attacks against vessels at sea and in port have occurred in a number of cases. The tanker Limburg was badly damaged off the coast of Yemen during an attack in 2002. A similar, but much less serious, incident occurred in July 2010 while the Japanese tanker M Star was passing through the Straits of Hormuz. In 2000, the American destroyer USS Cole was the target of an attack in the port of Aden, which resulted in 17 deaths. Historically, the greatest media attention has been directed at terrorist attacks against cruise ships, resulting in hostage situations. However, the consequences to society resulting from terror attacks in ports are more severe as not only the targeted vessel itself but also infrastructure of vital importance to society is affected.

### Systems for surveillance and security

Effective surveillance of open sea and ports requires that many different systems work in cooperation. Radar and optical systems operating together can be deployed to detect attempted thefts from anchored vessels. Indications of potential underwater activity can be obtained by deploying hydro-acoustic sensors. The need for collaboration between different sensor systems is further underlined by the fact that satellite systems are only capable of snapshots of activity during the actual satellite overflight, while ship- and land-based sensor systems are limited in their range to objects within their horizon. Furthermore, radar systems have limited capability to identify small objects on the surface of the sea, while optical systems cannot easily scan large areas quickly.

Current civilian sensor systems for marine use lack sufficient capability to detect and follow small objects on their own, especially on the high seas, in rain, or in darkness. If identification of objects is also required, the difficulty is even

greater. Vessels used for illegal activities are thus well able to hide from surveillance systems, especially if the vessels are small.

New methods with complementary technical systems acting in cooperation are needed for improved surveillance of pirates and smugglers at sea. Progress in technology for radar and electro-optical sensor systems has made possible the use of advanced sensor technology for the detection of small objects at sea. Sensor components previously used exclusively for military systems have become affordable and the rapid development of computer technology has made more advanced signal-processing techniques feasible for real-time use. These developments enable a more complete overview of vessel activity by combining information from the sensor systems with vessel positions from transponder systems such as AIS (Automatic Identification System). It should be noted, however, that small vessels often do not transmit AIS information and a complete overview of vessel activities also requires sensor systems on ships or along the coast that do not depend on vessel cooperation.

Trawlers and pleasure craft can be hard to distinguish from smugglers and pirate vessels, so sensor information needs to be accompanied by information from other sources. The administrative systems handling freight manifests, route planning, and customs declarations provide invaluable sources of information. These systems are being continuously developed and international bodies are constantly pushing for more efficient data handling and information exchange. Reports from customs inspections and other security personnel can result in immediate action, but information obtained in this manner can also be used in the development of automatic systems for threat detection. By means of comparison with a library of historical data or the results of scenario modelling, automatic systems can be "taught" to recognise threats or anomalies.

All new sensor systems generate large data flows. Raw sensor data need to be refined into concepts (such as "drifting vessel smaller than 8 metres") before meaningful integration with data collected from administrative systems to yield decision support information for operators. Automatic alarm functionality is needed when abnormal or unexpected situations occur, which in turn require the automated support systems to "understand" the information flow and collect only the most relevant information. In the long run, operators are then only faced with a limited number of alerts and decisions, instead of themselves having to continuously monitor the entire flow of information and detect anomalies manually.

### Remaining challenges

Despite the importance of well-functioning sea transport, there are still significant shortcomings in the efficiency and coordination of sea surveillance. Within the EU considerable effort is currently being directed towards the development of a contiguous and shared situational awareness along its coasts and in surrounding waters. The ambition of the Union is to improve security by forestalling cross-border crime.

In order to succeed, such work needs to be pursued at several levels simultaneously and with sufficient resources. Both technical systems and the climate of collaboration and political guidance need improvement. A system perspective is necessary in order to ensure that the available resources are being deployed in the most effective manner. As an example, a high fence paired with a video surveillance system provides no protection if criminals and terrorists can pass unchallenged through open gates because of corruption or negligence. It is important that the available resources are used where maximum effect can be achieved. At times this means a new sensor system and at other times a new routine for access or an organisational change that reduces the impact of corrupt employees.

In the technical arena, work at the EU level should be directed at developing improved, efficient and standardised technical solutions for vessel detection, information sharing and decision support. Here, the worldwide AIS system can serve as an inspiration. Research on technical solutions is collected over time into a standardised system, which is commercially refined and used everywhere. When the underlying sensor technology has reached a sufficient degree of maturity, work can proceed on standardisation of systems through international agreements. It is important that the development of technology goes hand in hand with standardisation efforts for the solution to be globally accepted both by commercial vendors and by end-users, especially when information is to be exchanged between operators.

The climate of collaboration between the various stakeholders involved in global shipping activities needs to be improved. In order for commercial operators to put efforts into collecting, verifying and sharing information, it is important that they receive some form of recognition or preferential treatment. Here, the example of the customs service can serve as an example. Faster clearance of goods can be given to shipping companies that provide complete and accurate information on upcoming shipments. Occasionally, the lack of willingness to share

information can be attributed to the risk of shared information getting into the wrong hands. Proprietary information cannot be allowed to reach competitors, and if information on route planning gets into the hands of criminals this can lead to thefts in the port area or even along highways far away from the ships and parts.

EU efforts should be focused on ensuring that adequate regulations exist and that sufficient governmental resources are made available. The development of training programmes and certification for personnel involved in the transport chain can also enhance trust between parties. Legal questions must be handled on a political level so that the information sharing can be handled in a manner that takes personal privacy into account. National security aspects must also be handled on the political level. One important question is how much data from military systems can be shared when analysis of such data can yield information about the performance of these systems.

Our open society is inherently vulnerable. Systematic work is needed so that limited security resources are used in a balanced way both to prevent incidents and to mitigate the consequences of the incidents that do happen. The EU and the Swedish Civil Contingencies Agency MSB are both interested in supporting work to improve the safety and security of sea transport. They are supporting research projects into sensor and decision support systems for safe and efficient sea transport. Trials and demonstrations will be conducted during the coming year with the port of Gothenburg among the locations chosen for the trials.

The collection and sharing of available information must take into account a number of demands and constraints, such as personal privacy, national security concerns, and the need to protect lives and property. At times these demands are at odds and changes in the political climate can also change the rules of the game. Modern sensor systems, voluntary information sharing and automatic decision support are needed so that the authorities and commercial operators can ensure the protection of international shipping, a keystone of the world economy.

## Further reading

http://ec.europa.eu/transport/modes/maritime/index_en.htm
http://www.supportproject.info/
http://www.seabilla.eu

# The EU and Star Wars: The Space Code of Conduct as a Tool for Security Policy

Eva Bernhardsdotter

*What do the diplomat at the Ministry for Foreign Affairs, the marine off the coast of Somalia and the mine worker in Kiruna have in common? They all depend on space services. What do the company Saab and the EU have in common? They are both promoting the use of a code of conduct as a means to manage activities and work in a responsible manner. The threefold role of the EU as an actor within the areas of security, space and arms control is manifested through the proposal for a space code of conduct in a context where the EU is using space as a tool for security policy. Sweden, like the EU, can contribute to the secure and sustainable use of space.*

The advent of arms control in space can be dated to the dawn of the space age when the Soviet Union in the late 1950s launched the first satellite the world had seen – Sputnik 1. With the launch of objects into space followed the military uses of space. The use of weapons in space is not a tale from Star Wars but is an established fact, as demonstrated by the superpowers on several occasions. The issue of an arms race in space has been debated bilaterally as well as in the UN. The characteristics of the space environment today contrast with the earlier days of the space age during the Cold War. Prestige space projects by the USA and the Soviet Union have been succeeded by congestion and competition in space as a result of the increasing number of space actors, governmental and commercial, and the growing amounts of space debris.

Space is increasingly contested due to the development of anti-satellite weapons. A placement and deployment of weapons in space would lead to strategic instability. This instability together with the growing volumes of space debris could prevent the use of space for national security purposes and global economic viability. Threats to the infrastructure in space are inextricably linked to national security as many states utilise satellites for intelligence purposes. Against this backdrop, and taking into account how increasingly dependent we are on space services, military and civilian users alike, several international initiatives have been launched to ensure the secure and sustainable use of space.

## What is a space code of conduct?

The deadlock in the UN on the issue of arms control in space and the Chinese test of an anti-satellite weapon in 2007 acted as catalysts for

the EU's involvement in this issue. The proposal for a code of conduct for outer space was formulated in the working group CODUN Space, a group that was set up in 2007 to manage the code. CODUN Space is a subgroup of the EU working group CODUN (Committee on Disarmament in the United Nations), which deals with disarmament issues. The code is an agreement between subscribing states to adhere to a set of guidelines when conducting space activities, with the aim of achieving a secure and sustainable use of space. Similar agreements exist, for example for incidents at sea. The code is politically binding, meaning that the subscribing states make a political commitment to follow the guidelines in the text.

The preamble describes the motivation behind the code and highlights the benefits of space services. The following four chapters of the code contain the general principles to guide subscribing states, measures on space operations and various cooperation mechanisms. Organisational guidelines are also included as the code is managed outside the UN system. Specifically, subscribing states commit themselves to refrain from destroying or damaging other space objects and from deliberately creating space debris, unless it is justified by the right to self-defence under the UN Charter. Furthermore, the code encourages notification of space activities to and sharing of space policies with other states in order to promote transparency. Subscribing states also commit themselves to adhere to the international legal framework for outer space.

The modern governance of space activities must be comprehensive as civilian and military space issues are converging. International space law is to some extent outdated and does not consider space debris or developments in technology, while the code does. Specifically, the code focuses on the desired effect – security in space – rather than banning specific threats, such as which types of weapons to ban. The code therefore cleverly avoids the issue of how to define a space weapon, a dilemma that has often featured in the international discourse on space and arms control.

As a multilateral initiative, the code not only raises awareness of space security and sustainability but also engages the political will to prevent space from becoming an arena of conflict as a result of mishaps and misunderstanding. The code elicits support in the highest political echelons in states regardless of size: for example; the USA and Australia officially showed their support for the initiative in 2012.

### The threefold role the EU plays in security, space and arms control

The code can be viewed as a national security tool that strengthens the threefold role of the EU as a global actor within the fields of security, space and arms control. As the recipient of the 2012 Nobel Peace Prize, the EU has many expectations to fulfil.

When the Lisbon Treaty entered into force in 2009, the EU's competence over space matters was established, and hence its role as a space actor as well. Space capabilities contribute to social and economic development as well as security in Europe and may be used for political purposes. The flagship programmes Copernicus (earth observation for environment and security) and Galileo (the European satellite navigation system) demonstrate the key role space capabilities play in the EU Common Security and Defence Policy.

The importance of space capabilities for national security in Europe is recognised today. Nevertheless, the EU, and the space nations in Europe, lack a comprehensive strategy that addresses the antagonistic threats to the infrastructure in space, a vital strategic asset, and the role of the EU as a space power. The issue of space security is complicated by the many actors in Europe, where some countries are more prominent as space actors than others. The role of the EU as an actor in security is emerging and is reflected in the European Security Strategy, where today's complex threats are addressed with "soft" power tools such as prevention and assurance rather than by purely military means. The code mimics the principles of preventive and broad measures, as well as multilateral cooperation encapsulated in the security strategy.

While it is not an arms control treaty per se, the code is being managed within the disarmament and non-proliferation community in the EU. The establishment of the Common Foreign and Security Policy, through the 1992 Treaty of Maastricht, led to the emergence of the EU as a disarmament and non-proliferation actor. Today, the EU is an actor of good repute in this area, and the code, an EU-led initiative, is vital in upholding this reputation.

### Sweden and the space code of conduct

In order for the EU to appear as a credible actor, the member states must be clearly guided in the same direction as the EU. For Sweden, as a de facto space nation and having participated actively in the drafting of the code, subscribing to the code would entail a confidence-building measure, communicating Sweden's commitment to the secure and sustainable use of space.

Securing the infrastructure in space is a priority for all users of space services today, and the code is therefore a matter of concern for every citizen of Sweden. Additionally, Sweden conducts space activities and has launched several satellites into space. Subscribing to the code would affect these activities in more than one way and would have consequences for government agencies as well as commercial satellite operators. Implementing the provisions in the code specifically entails a commitment to avoid collisions in orbit and the creation of debris, but also to notify other states of events that may affect their space objects. In order to ensure the efficacy of the code, the subscribing states must be engaged in building confidence. In view of this, it would be costly, in political terms, for Sweden to subscribe without abiding by the new commitments the code would entail.

The issue of space security is a matter for the Swedish Ministry for Foreign Affairs; however, these activities are not closely linked to those of other Swedish government space actors. Sweden lacks a single appointed entity with the mandate to manage space capabilities for defence and security. The lacunae in the national governance of space matters are aptly highlighted in the audit report, published in 2013, on Swedish space activities by the Swedish National Audit Office. The report states that the administration of space matters is fragmentary and that there is no comprehensive overview of the space activities.

### Warning bells are ringing

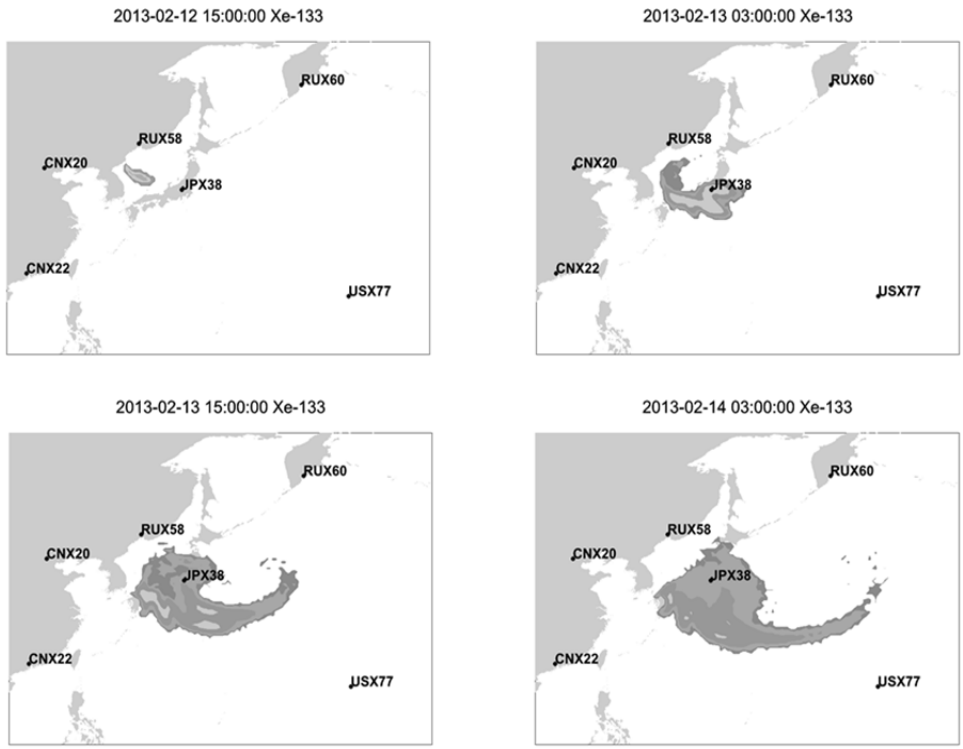
During the Swedish presidency of the EU in 2009, Sweden chaired the working group managing the code. Since 2010, the European External Action Service has taken over as the chair, thereby providing the impetus for the code rather than the member state holding the presidency. The code is a priority item on the EU agenda and expectations on the EU are high that the EU will soon produce an internationally acceptable draft text and arrange a diplomatic conference where states and organisations can subscribe to the code. The initiative has not, however, entirely been welcomed with open arms outside the EU. Both the contents of the code and the process have been criticised.

Diametrically opposed opinions on the code have been voiced: on one hand the legally non-binding code lacks teeth; on the other hand the guidelines in the code may in time develop into legally binding measures. There is also concern that the adoption of a code will reduce the incentives for a treaty banning weapons in space. For those states advocating such a legally binding treaty the code poses a challenge.

While the content of the code has been hammered out, it is the process of the code rather than the content that poses the greatest challenge for the EU. The Hague code of conduct against the

proliferation of ballistic missiles is a prime example of a multilateral initiative outside the UN system. Notwithstanding this, the fact that the space code of conduct is managed outside the UN is a source of criticism, particularly for states like Russia, China and Pakistan. In the UN, civilian and military space issues are addressed separately, making it difficult to find a suitable forum in which to discuss the code, which concerns all types of activities in space. The EU must rise to the occasion and manage the code outside the UN, while at the same time maintaining the multilateral character of the process to avoid giving the impression that the code is a Western ploy. The lack of a concrete road map for the process has further eroded the initiative. Official statements about multilateral meetings which are then postponed put a strain on the EU's reputation, but on the other hand the date and location for such meetings must be carefully selected.

The EU is on a precarious footing. In order to be perceived as a credible actor in its threefold role on the global arena, it must speed up the process and lay out a road map. Furthermore, the EU has to walk a fine line between drafting a code that is acceptable to most states and actors, and delivering a code that is relevant for security in space. It is not simply the reputation of the EU and its potential for soft power that are at stake, but also the growing awareness of the secure and sustainable use of space. Space debris and the use of weapons against the space infrastructure are the foremost and urgent challenges. The international discourse on the code and space security has gained momentum during the past six years, but there is a risk that the engagement is waning. As an EU member state, Sweden is involved in the initiative for the space code of conduct. As a space nation, Sweden is also expected to contribute to the international effort for space security. Sweden must therefore begin to view space capabilities as a strategic resource and abandon the antediluvian mindset on space matters in favour of a more comprehensive overview.




Atmospheric transport calculation showing how a prompt release of the noble gas xenon from the North Korean nuclear test on 12 February 2013 would have been transported in the atmosphere during the ensuing two days. The markers show the locations of CTBTO monitoring stations in the region. The stations at Guangzhou in China (CNX22), Takasaki in Japan (JPX38) and Wake Island (USX77) are equipped with the Swedish SAUNA system which was developed by FOI. The calculation demonstrates that the station in Japan (JPX38) would have been hit by the cloud. Together with data from this station, the calculation can be used to show that, if noble gases leaked during the first hours following the explosion, the leak must have been less than about 0.01% of the total amount produced. (Source: FOI)

# International Monitoring of Nuclear Testing: The Example of North Korea

Anders Axelsson, Niklas Brännström, Anders Ringbom and Pontus von Schoenberg

*The North Korean nuclear test carried out in February 2013 once more brought attention to the Swedish and international capability to detect and study nuclear test explosions. This capability has increased significantly since the turn of the century, and can be used both to determine whether a nuclear explosion has occurred and to gather information about the explosion, e.g. about the type of device.*

After the end of the Cold War, the relevance of nuclear weapons has changed but hardly decreased. Nuclear arms continue to play an important role for established nuclear weapon states, while at the same time the number of actors is increasing. Several new states have acquired or are suspected of making efforts to acquire nuclear weapons. International efforts to limit the proliferation and development of nuclear weapons require credible verification. It is for example important to be able to detect clandestine nuclear weapons-related activities such as nuclear test explosions, reactor operations or reprocessing of irradiated nuclear fuel.

North Korea's actions demonstrate how nuclear testing can also be used for political purposes, and it is therefore important for the international community to gather the best possible knowledge about what actually occurred and how it should be evaluated. The capability to detect and study nuclear explosions has increased significantly in the past 15 years. The primary reason for this is the construction of the international monitoring system to verify the Comprehensive Nuclear Test-Ban Treaty (CTBT), which is not yet in force. The system offers states that do not have their own resources for detecting and measuring nuclear explosions the opportunity to acquire first-hand knowledge about events such as the recent North Korean nuclear test.

With the right technical analysis capability a small state such as Sweden can also make important contributions to international verification in the nuclear weapons field. There is good reason to

reflect on several issues related to this. What can be measured? What is the impact of this development on the credibility of the CTBT and on the likelihood that it will eventually enter into force? Are there conclusions to be drawn from a verification point of view after North Korea's latest nuclear test? How are the deliberations and actions of North Korea or other states that may want to conduct nuclear tests in the future affected?

### What can we measure and what conclusions may be drawn?

Nuclear explosions on the ground or underground, cause seismic waves that may be detected over great distances. Generally speaking, sensors in the same region (at distances of hundreds or a few thousand kilometres) are most important, but sensors at a greater distance may also contribute information. Networks of a larger number of sensors are most effective. Explosions in the atmosphere or under water also generate waves that can be detected by infrasound and hydro-acoustic methods, respectively. Analysis of seismic signals gives information on such factors as time, location and explosive yield. It is also possible to distinguish between earthquakes and explosions. As in all data analysis, there are uncertainties in the information that is obtained. The difficulty in confidently distinguishing an explosion from an earthquake or in accurately estimating the location or explosive yield will vary depending on various factors such as explosive yield and local and regional conditions.

Nuclear explosions also produce large quantities of radioactive materials that can be dispersed in the atmosphere, transported over great distances and detected by measurement stations that collect samples from the air. For this to work a sufficient amount of such radionuclides must leak from the test site, and atmospheric conditions must be such that they are transported in sufficient concentrations to one or more measuring locations. The probability of leakages from underground nuclear tests occurring is difficult to estimate. Experience from past testing by the nuclear weapon states suggests that minor leaks were not uncommon. The efforts made by the nuclear weapon states at the time to contain radionuclides were aimed primarily at avoiding radionuclides that could be harmful to health leaking out into the environment, not at concealing a test. It is likely that more efficient containment can be achieved if it is a priority of (e.g.) North Korea, but on the other hand it should be difficult even with great effort completely to ensure non-leakage of the very small amounts that are required for off-site detection. It is generally assumed that the noble gases, such as krypton and xenon, would be most likely to leak.

The likelihood of radionuclides being detected is of course also affected by weather conditions during and after a leak. The greater the leak the greater the likelihood that measurable quantities of radionuclides will reach a given measurement station, and the more sensitive the measurement station the smaller the quantities required. However, if the wind is blowing in the wrong direction even extremely sensitive measuring equipment will not suffice. To reach a high probability of released radionuclides being detected regardless of the weather, a network of measurement stations at suitable distances from each other is required.

Analysis of radionuclide data may aim to detect or confirm a nuclear explosion, or it may aim to gather further information on the event. To detect or confirm an explosion, the source of the radionuclides detected in one or more measurements must be located in time and space. This can be done using atmospheric dispersion modelling that uses data from global weather forecasting models – an "inverse" calculation is made to delimit the area from which the radionuclides measured may originate. To get a better verification of events it is also possible to do a "forward" calculation from a hypothetical source. Ideally, the location, size and time profile of a source may be determined. However, the analysis is complicated not only by uncertainties in modelling and measurements but also by the fact that not only nuclear explosions release small amounts of radionuclides into the atmosphere; nuclear reactors and medical isotope production facilities, for example, also do so.

The ratio between radionuclide concentrations that are measured may provide further information that may help delimit the nature of the source and the time of an explosion or other release. Depending on the measurement results, this sort of analysis may be extended to yield more detailed information on the device and thecourse of events.

### The Comprehensive Nuclear Test-Ban Treaty

The CTBT, which was opened for signature in 1996, prohibits all nuclear explosions. States that sign this type of treaty must, after completing the necessary legal arrangements (e.g. decisions in their legislative assemblies), confirm or ratify that they regard the treaty as legally binding. Sweden ratified the CTBT in 1998. So far, 183 states have signed and 159 states have ratified the CTBT. For the treaty to enter into force the ratifications of 44 named states (the so-called Annex II states) are required. Eight of these states have not yet ratified: China, Egypt, India, Iran, Israel, North Korea, Pakistan and the USA. Of the eight,

India, North Korea and Pakistan have not yet signed the treaty. The process for the CTBT to enter into force is a slow one: with one exception (Indonesia in 2012), all ratifications so far among the Annex II states were received in 2004 or earlier, in most cases before 2000. This extended process may eventually result in signatory states questioning the obligations they have undertaken in regard to, e.g., construction and operation of the verification system. The decision of the USA is a key issue for continued broad acceptance of the CTBT, and for the USA the discussion on whether or not to ratify the CTBT is partly about whether the desired nuclear capabilities can be maintained indefinitely without testing, and partly about whether how effective verification of the treaty will be.

The most current issue surrounding the CTBT is therefore not that it can be expected to enter into force in the near future, but rather the comprehensive technical verification regime that is being constructed. The system has achieved a considerable capability in recent years. It consists of a global network of monitoring stations that collect data by the several different measurement technologies discussed above. Measurement data are forwarded via an international data centre in Vienna to the member states of the Comprehensive Nuclear Test-Ban Treaty (CTBTO) Preparatory Commission, the organisation charged with preparing for implementation of the CTBT. The means therefore exist for any state to acquire good first-hand information on nuclear testing or similar events in principle anywhere on the planet.

The CTBT places the responsibility for detecting possible treaty violations through analysis of data from the network on the member states. In other words, verification is in the hands of the member states in a quite different and more direct way than is the case with e.g. the 1968 Treaty on the Non-Proliferation of Nuclear Weapons (NPT), where data are handled and analysed within the International Atomic Energy Agency (IAEA), which then communicates its conclusions to the member states. For credible verification of the CTBT, therefore, many member states must have the ability to independently evaluate the data collected. The credibility thus built is in turn a factor that may play a large role in determining whether the USA especially will decide to ratify the treaty.

### North Korea's nuclear test in February 2013

The North Korean nuclear test on 12 February 2013 was expected, and readiness to receive and analyse measurement data was high around the world, not least at FOI, which operates

the Swedish National Data Centre for CTBT verification. FOI has also developed both equipment and analysis methods that are employed in the CTBT verification system. The test was carried out early in the morning (Swedish time) and after about five hours FOI reported its assessment that a nuclear test had been conducted, including the time, location and estimated explosive yield (the equivalent of between 10,000 and 20,000 tons of TNT), based on seismic signals detected by the international monitoring network. Detailed analysis of radionuclide measurement data, including meteorological dispersion models and comparison with normally occurring observations in the region, was still ongoing in May 2013 at FOI as well as other places around the world. The illustration shows an example of a calculation. It is probable that some of the detections of radioactive xenon that have been made can be connected to the test, but it is clear that immediate releases, if any, were small and that measurement data will not allow detailed conclusions on e.g. the type of material (uranium or plutonium) used in the device.

From these results, different conclusions can be drawn. Seismic measurements have evidently functioned satisfactorily and are expected to be the prime source of information on the location of any nuclear weapons test. From the point of view of CTBT verification, the primary aim of radionuclide measurements is to confirm that the seismic signals came from a nuclear test, and not from any other sort of explosion or from an earthquake. In the case at hand, other sources of the seismic signals can be excluded, primarily due to the size of the explosion. Generally speaking, the situation could be more complicated, and ambiguous seismic results could need confirmation through radionuclide measurements.

Such a measurement was carried out by FOI in 2006, when we were able to confirm the first North Korean nuclear test by a measurement in South Korea. To provide such a result, the source of the radionuclides being measured must be located, at least roughly, and this is done by modelling the dispersion of radionuclides in the atmosphere. The method is most effective if radionuclides from the same source can be detected in several measurements, at several measurement stations. Given the planned density of the network, however, it is not likely that more than one station will detect a minor release. It is also important not only to detect but also to measure concentrations that are high enough to allow conclusions on the source of radionuclides. For these reasons, it now appears important that states with an interest in effective monitoring,

perhaps in selected regions, complement the network with additional measurement stations or mobile measurements of the type undertaken by both Japan and South Korea immediately following the recent North Korean nuclear test.

Sharing of data from such national measures with other CTBTO member states could significantly strengthen the capability of the network to detect and evaluate nuclear weapons tests. The evidently small size of any releases from North Korea's recent nuclear test could be due to special efforts by the country to avoid even minor, non-hazardous releases. Such efforts would not, in the case of North Korea, aim to hide the test itself, at least not this time. One reason could be North Korea's trying to obstruct the sort of technical analysis which we have briefly described.

## The role of Sweden

Verification of the CTBT is organised in a manner that leaves great responsibility with the CTBTO member states, and also gives them access to first-hand information on relevant events globally. Sweden has played an important role in the development of technology and methods for CTBT monitoring, especially in the radionuclide field, where FOI has developed SAUNA, an automatic system for collection and measurement of radioactive xenon from the air. Sweden also contributed in a major way to nuclear explosion monitoring before the CTBT, e.g. by detection of seismic signals and airborne radionuclides mostly from atmospheric nuclear testing. The international network which is now becoming available provides greatly enhanced possibilities to detect and analyse nuclear tests anywhere in the world, even underground or under water. In connection with North Korea's recent and possible future nuclear tests, smaller states such as Sweden will play an important role and share responsibility in the technical assessment of what has occurred.

## Further reading

Ringbom, Anders; Elmgren, Klas; Lindh, Karin (2007) *Analysis of Radioxenon in Ground Level Air Sampled in the Republic of South Korea on October 11–14, 2006*. FOI-R--2273--SE.

Baklanov A, Mahura A, Jaffe D, Thaning L, Bergman R, Andres R (2004) *Atmospheric transport patterns and possible consequences for the European North after a nuclear accident*, FOI-S--0039--SE.

# Rare Earth Elements and Europe's Dependence on China

Malek Khan, Martin Lundmark and Jerker Hellström

*Rare earth elements (REEs) are used to produce mobile phones, X-ray machines, nuclear power plants and many other high-tech applications. Without access to REEs, industry would not be able to produce a range of products with cutting-edge features. About 95 per cent of all REEs comes from mines in China. Officials in many European states regard this dependence on a single source of an important resource as an undesirable uncertainty. Moreover, a large part of the components containing rare earths are also produced in China. As a result, government and business actors will not substantially reduce their dependence on REEs from China merely by securing access to raw materials from alternative sources.*

There are 17 rare earth elements, of which several were discovered in Sweden in the 18th and early 19th centuries. Five of them were discovered in Ytterby in the Stockholm archipelago, as is evidenced by their names: yttrium, terbium, ytterbium, erbium and holmium (after Stockholm). It is also in Sweden that the EU's main potential REE deposit is located, in Norra Kärr outside Gränna in the southern part of the country.

Demand for REEs has increased in recent years, partly because of their relevance for systems that have been developed to reduce human impact on the environment, such as wind turbines and electric cars. However, these metals can also be seen as a strategic resource, as the defence industry needs components containing REEs in order to produce missiles, smart bombs, fighter jets and other high-tech equipment. REEs are important for the production of high-performance electric motors, magnets and sensors, as well as in guided munitions and electronic warfare. Components containing REEs often have better performance, are smaller and more durable, and can withstand extreme temperatures and pressure better than conventional alternatives. This has made REEs interesting for the development of defence applications. The United States was the dominant producer of REEs until the mid-1980s, when it was overtaken by China due to its ability to produce REEs at significantly lower cost at a time when international demand was increasing. China, however, had begun extracting REEs as part of its iron and steel production as early as the late 1950s.

With 95 per cent of global production, China is by far the largest supplier of REEs. It is also the world's largest REE consumer, due to the fact that components containing REEs are mainly produced

in the country. The establishment of a strong Chinese component industry is mainly a result of the general globalisation trend that has moved much of advanced production from the USA and Europe to Asia. Out of the 17 rare earth elements, only five are characterised by a potential dependency problem: neodymium, terbium, europium, yttrium and dysprosium.

Against the backdrop of growing Chinese demand and China's increasing control over the international supply, industry officials outside China have begun to ponder how this may affect access to REEs in other parts of the world. China adopted export quotas on REEs in 2004, and caused some international concern when quotas were reduced significantly in 2010. Some of the strongest reactions came from Japan, the world's largest importer of rare earths. In July 2012, the World Trade Organization (WTO) launched an investigation into China's REE export quotas, as suggested by Japan, the US and the EU. If the WTO concludes that China is in breach of the trade body's regulations, it may have to lift its export quotas.

A major motivation for the Chinese export quotas is that they are needed in order to come to grips with the serious environmental damage that the REE industry is causing today. Indeed, if the costs of environmental clean-up are taken into account, it is clear that China would not be able to sell REEs at the current low price levels. The prospect of limited and more expensive exports from China is an incentive for REE consumers internationally to secure access to REE resources from other sources. Exploration is, in fact, being carried out all over the world, and there are promising deposits in Greenland, Sweden, Kazakhstan and Kyrgyzstan, as well as on the Pacific seabed off Japan. China might also see the establishment of other sources of REEs as a positive development, considering that it is itself a major consumer of REEs and the fact that it may become a major importer of REEs in the future.

### Defence industries and REEs

REEs are one of the resources for which European defence firms are most dependent on overseas suppliers, as revealed in a study led by FOI in 2012. The companies that participated in the study believed that this dependence carried with it potentially large and uncontrollable risks – risks that will increase in the future. Some of the defence firms' product designs are based on features that can only be achieved with REEs, meaning that the REEs cannot be replaced without products losing in performance.

In order to solve the problem of dependence on REEs, it is not enough to secure access to REE raw materials from countries other than China: each step in the production chain needs to be reviewed.

In addition to ensuring access to the raw material – either through mining or through recycling – there is a need for a process industry that can take care of the raw material and process it into useful alloys. In addition, deliveries must be secured of the necessary REE components for the defence industry.

In Europe, there are currently neither any commercial REE mines nor any facilities for processing the raw material. The only potential deposit within the EU is at the above-mentioned Norra Kärr, which is in the exploration phase. Exploratory drilling indicates that there are commercially interesting amounts of dysprosium in particular. Mining rights to Norra Kärr are owned by the Canadian company Tasman Metals. The firm announced in February 2013 that it also had an REE deposit in Olserum, about 100 km east of Norra Kärr.

Currently, there is also no viable industry for recycling of REEs, despite the environmental aspects of recycling of resources and the problems regarding strategic dependency. REEs could potentially be recovered from collected electronic waste, municipal and industrial junkyards, waste from old mines and waste materials from industrial production. In principle, metals can be recycled infinitely, yet in practice the recovery of REEs is often ineffective or non-existent due to limitations in product design, recycling technology and know-how about the separation of metals.

There is at present a lack of technologies and processes for REE recycling in Europe. A large part of the electronic waste from the EU and the United States is currently exported to countries in Africa and Asia. In order to be able to establish a process for recycling rare earths in Europe, there is among other things a need for adequate logistics for the management of recycled materials and a structure that simplifies and encourages recycling, but also a need for more in-depth research concerning separation of the desired metals. In a long-term perspective, it is uncertain whether Europe will have an adequate chemical process industry that can process material containing REEs from mines and recycling.

The last link in the production chain – the processing of REEs into components – is no longer based in the USA and Europe, despite the fact that this is often where the products that require such components are designed. Instead, the material is processed in the vicinity of REE mines, which tend to be located in China. At present, few nations possess the capacity that is needed to produce low-cost electronic components, on a large scale, that are in demand globally. Thus there is a dependency problem further down the value chain, in terms of demand for raw material, as well as further up, in terms of component production.

### Mitigation strategies for addressing rare earth element dependency

From the perspective of national security, the US is the country most concerned with China's dominance where REEs are concerned. In order to reduce the American dependence on China, mining of REEs was resumed in 2012 at the Mountain Pass rare earth mine in California. There are also suggestions that the USA should recreate the entire value chain, from mining to strategically important components.

In June 2010, the European Commission published a report on critical minerals. The report points to possible issues that could cause disruption in production and supply chains in Europe and globally. REE are described as critical for the EU's economic and industrial development. Countries within the EU have different strategies for dealing with the REE issue and there is still no uniform policy.

Germany and Japan are two countries with large REE-dependent manufacturing industries and they have identified potential industrial and political risks in relying on China as the dominant supplier of REE raw material. Both countries are therefore looking for alternative ways to get access to REEs, such as through alliances with other countries. In 2012, the German government signed a strategic cooperation agreement with Kazakhstan regarding mining of REEs. In the same year the German state enabled, by direct aid, the establishment of the company Deutsche Rohstoff AG (DRAG), which will work to secure REEs for German companies. In much the same way, Japanese companies are involved in Russia and are also trying to tie in potential suppliers in Vietnam, Kazakhstan, Australia and Brazil.

In France, the Committee for Strategic Metals has concluded that the supply of REEs will be crucial for the industrial and energy sectors; however, no tangible action has been taken. The French government believes that recycling of certain metals should be viewed as a strategic resource. The United Kingdom differs by emphasising free trade agreements and market mechanisms. For Russia, REEs do not appear to be a major problem today. The Russian electronic component industry is at a lower level of sophistication and, in addition, state-controlled defence companies mainly purchase electronic components from other state-supported producers. While Russia currently lacks an REE industry, there are detailed plans for how to satisfy future military and civilian demand from domestic resources.

In summary, countries that are dependent on REEs for their industry or defence technology development can choose to promote free trade, combat abuse of market dominance, collaborate with other

states on research on REEs, work to establish bilateral agreements with countries with access to REEs, or establish vital assets within their own control.

In the foreseeable future, recycling aimed at increasing the supply of REEs will mainly be pursued on the national level. Meanwhile, the recycling of electronic goods is likely to be more efficient using large-scale solutions, which points towards the possible establishment of centralised processes in Europe. Some countries, including Sweden, have also established cooperative projects regarding REE recycling with China.

Going forward, it is likely that some EU countries will establish new partnerships with mining companies and industries overseas in order to diversify their access to REE raw material and components. Major economies such as France and the USA may launch partnerships with countries outside China, in the same way as Germany has done with Kazakhstan. It will also become increasingly important to invest in research on REEs, including recycling, substitute products and sustainable production. As recycling matures and becomes more efficient, coordination between EU member states could become important in order to realise economies of scale.

### Demand for REEs in the future

In the short term, China's control over global access to REEs will remain. This is not a problem at present; industry has access to the minerals and components it needs and at reasonable prices. Rather, it is the potential risk of denial of access to REEs in the longer term that is seen as problematic.

REEs are a resource that is only needed in small quantities, but still has unique features. Due to the limited demand for REEs, global prices tend to be volatile and it cannot be taken for granted that REE mines (or REE recycling) will be profitable in the long run. This uncertainty is a clear obstacle to establishing new mines and processing plants outside China. States or industries will only make such large investments if they have identified a significant strategic need to reduce their dependence on REE imports. Recently, two mines have reopened in the USA and Australia – Mountain Pass and Mount Weld. These operations have experienced profitability problems, in part due to lower demand resulting from the global economic downturn.

With its model of state capitalism, China may be able to cope better with issues regarding REEs in the long run. Hence there is a clear risk that the rest of the world will be dependent on China for years to come. Mineral deposits outside China is not going to solve the

dependence problem, unless the issue of profitability is successfully addressed. Moreover, in order to drastically reduce dependence on a single supplier, it is not sufficient to secure access to REE raw material – there must also be strategies in place to ensure access to the required components containing rare earths.

In conclusion, component manufacturing will remain outside European control. Since there is no commercial basis for the concentration of the entire value chain in Europe, European defence industries will have to adapt to dependence on China. If this dependence is seen as problematic from a security policy perspective, there could be a case for promoting the production of REE components in the EU. Today, this comes across as an unlikely scenario, but it is only when it becomes a reality that deposits such as Norra Kärr could come to play a strategic role.

### For further reading

European Commission (2010) *Critical Raw Materials for the EU*.

# About the Authors

**Anders Axelsson** holds a PhD in Nuclear Physics and is a Senior Scientist at the unit for nuclear weapons issues at FOI. He works primarily in the field of technical verification and is a project manager for the Swedish National Data Centre (NDC) for verification of the Comprehensive Nuclear-Test-Ban Treaty (CTBT). He has been developing equipment and methods at the Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO) and is also a former analyst at the IAEA Department of Safeguards.

**Eva Bernhardsdotter,** PhD, is the project manager for Space and Arms Control at FOI and specialises in issues relating to space, security and defence. She provides expertise to the Swedish Ministry for Foreign Affairs on arms control in space and space security. She is also serving as a technical expert in the EU-initiated efforts for a Space Code of Conduct. Previously she has worked at NASA and for the Swedish Space Corporation in the areas of microgravity and astrobiology research as well as satellite mission design.

**Niklas Brännström** holds a PhD in Mathematics and is a researcher at FOI's unit for dispersion calculation. Niklas works mainly on mathematical inverse modelling applied to atmospheric dispersion problems. His interests are mathematics, physics, dynamical systems and mathematical modelling.

**Kristoffer Darin Mattsson** is an analyst at FOI's Division for CBRN (Chemical, Biological, Radiological and Nuclear) Defence and Security. He has degrees in Geography and International Relations and is working in the field of sustainable security with environmental assessments, primarily from an international operation and climate change perspective. He has previously worked in Brussels with environmental and energy issues related to the EU's Common Agricultural Policy.

**Markus Derblom** is the Department Head for Peace Support Operations at FOI. His previous assignments include project management, advisory roles and studies in fields such as military doctrine, civil-military relations, strategic and operational-level command, the evaluation of peace operations, and African security. Markus has a background in Political Science from Uppsala University, with a Master's degree in Political Psychology and International Politics.

**Amanda Eriksson** holds a Master's degree in Economics and studied Economic History. She works as an analyst in FOI's unit for logistics, personnel and economics. Currently she is providing analytical support to the armed forces in the management staff and works there mainly with monitoring and analysis.

**Jerker Hellström** is an East Asia analyst on the FOI Asia Security Studies Programme. He mainly studies issues regarding China and the Korean Peninsula. His previous research at FOI has involved topics including Sino-Indian relations, the Chinese presence in Africa and the EU arms embargo on China. Jerker was the Chief Editor of Strategic Outlook 2011 and previously worked for Reuters as a correspondent in Stockholm and Shanghai.

**Ulrik Franke** works as a scientist at FOI's Department of Information and Aeronautical Systems and has a PhD in Industrial Information and Control Systems. He is the project manager of the cross-disciplinary project National Security in the Information Society, which investigates the interaction between politics and information technology. Ulrik is also an officer in the Swedish Army reserve, with service both on missions abroad and in the Armed Forces Headquarters.

**Elisabet Frithz,** PhD, has previously conducted research in bacterial pathogenicity and is now working with nonproliferation issues. Elisabet supports the Ministry for Foreign Affairs on issues relating to the Biological Weapons Convention and has a focus on scientific and technological developments in lifescience.

**Cecilia Hull Wiklund** is as an analyst specialising in peace support operations. Her work has involved civil-military cooperation in peace operations and the UN peacekeeping system. She also works on issues pertaining to African peace and security, particularly regional security cooperation and African-led peacekeeping. Cecilia holds a Master's degree in International Studies in Peace and Conflict Resolution from the University of Queensland, Australia, and has, among other things, worked as a peacekeeping evaluation consultant for the UN.

**Malin Ivarsson** holds an MSc in Economics and has also studied Political Science. She works as an analyst at the Division for Defence Analysis, FOI. She is project manager for an operation analysis group, located at the Swedish Armed Forces Headquarters, which works mainly with questions regarding the Swedish Armed Forces' transformation from a conscript to an all-volunteer force.

**Sören Jägerhök** heads FOI's contribution to the EU-financed harbour security project SUPPORT. At FOI's Sensor and EW (Electronic Warfare) Systems Department, he has several leading roles within EU projects relating to the detection of abnormal behaviour, port security, container security and safety at temporary events. Due to his interest in marine applications, in the 1980s Sören obtained a diver's licence and served as a secretary in the joint programme for Sea Technology of the Swedish Board for Technological Development and the Defence Research Establishment (today's FOI).

**Malek Khan** started his research career as a theoretical chemist doing large-scale simulations of polymers and DNA. After his PhD he worked in academia before joining FOI. Malek is currently supporting the Plans and Policy Department at the Swedish Armed Forces Headquarters as an operations analyst. He also works with non-dependence issues regarding how Europe can ensure access to materiel and skills essential for military and civil security. Malek has received the Ingvar Carlsson Award for his research.

**Björn Larsson** is Deputy Research Director with a focus on radar systems. He joined the Defence Research Establishment (today's FOI) in 1980 and headed the ICERAD project developing new methods for the detection of "growlers" in Arctic waters in the mid-1980s. The methods were tested in sea trials in the Arctic. Björn has been involved in FOI's programme for low-frequency synthetic aperture radar (SAR) for several years and was the Head of the Department for Radar Systems in 2001–2009. Recently he has also been working as project manager for different EU projects.

**Birgitta Liljedahl** is a Senior Analyst at FOI's Division for CBRN Defence and Security. She heads FOI's support to the Swedish Armed Forces regarding medical intelligence for international operations and coordinates cooperation between Sweden and the UN in the area of environmental and health risks in peacekeeping. She has conducted environmental investigations in Kosovo, the Democratic Republic of Congo (DRC) and South Sudan. Birgitta has also been seconded as an environmental expert after natural disasters in Haiti and Kenya.

**Per Lind** holds a PhD in Organic Chemistry and is a researcher at FOI's Division for CBRN Defence and Security. Per works with laboratory issues concerning chemical munitions but also with theoretical studies and analyses of the impact of technological progress on threat assessments. For several years he has been working on issues related to export control and non-proliferation as well as to the Chemical Weapons Convention.

**David Lindahl** holds an MSc in Computer Science, and works with research into IT security and cyberwarfare at FOI. He has lectured and taught classes to military units, government agencies and civilian corporations about the opportunities and risks associated with computer systems. David has also participated in the creation of the NCS3 Lab, the national Swedish programme for security in computer-controlled critical infrastructure. In that project he is now responsible for courses and lectures for corporations within among others the power, water and transport sectors.

**Martin Lundmark** is Deputy Research Director at FOI's Division of Defence Analysis. He has a degree as Doctor of Business Administration from the Stockholm School of Economics. He has worked with FOI since 1998, and his foremost areas of expertise are the defence industry, defence materiel acquisition, arms exports and strategy implementation. He has been a guest researcher at the Security Studies Program, MIT in Boston, and at the Fondation pour la Recherche Stratégique in Paris.

**Lena Molin** has a PhD in Economic History from Stockholm University. She conducts research in the fields of veteran affairs and food safety and heads FOI's Veteran Statistics project. Lena also contributes to food-related projects at FOI and at the Royal Swedish Academy of Agriculture and Forestry.

**Claes Nilsson** is an analyst specialising in peace support operations. His research has involved different aspects of crisis management, ranging from humanitarian aid to civil-military cooperation and security sector reform. Among other things, Claes has studied the conflict in Afghanistan and the Swedish engagement in the country. Previously, he held the position of project manager for FOI's Peace Support Operations studies, with special attention to evaluation of operations.

**Johan Norberg**, is a senior researcher with an MSc in Russian and Business Administration, and has studied at St Petersburg's Institute of Finance and Economy. His research at FOI covers developments in Russia with a focus on the Armed Forces. He has also analysed international operations of the Swedish Armed Forces, mainly related to Somalia. Johan has worked in the Swedish Ministry of Defence, the Ministry for Foreign Affairs and the Swedish Parliament and served as an officer in Swedish peacekeeping operations in Bosnia, Georgia and the Middle East.

**Rolf Ragnarsson** has been a researcher in the Radar Systems unit of FOI since 2009. His current work deals predominantly with issues surrounding the development of sensor systems for maritime safety and surveillance and with imaging bistatic radar systems. He has also worked in industrial development of radar systems for traffic applications as project manager and systems engineer, and as a researcher in condensed matter physics at Cornell University in the USA.

**Anders Ringbom**, holds a PhD in Nuclear Physics and is Deputy Research Director at the unit for nuclear weapons issues at FOI. Anders has worked in the field of development of nuclear verification techniques at FOI since 1998. He also acts as technical expert in the area of nuclear treaty verification, in particular in the establishment of the verification regime for the Comprehensive Nuclear-Test-Ban Treaty (CTBT). He is a former project manager for the SAUNA detection system, which is being used worldwide for the detection of radioactive noble gas releases from nuclear tests.

**Steven Savage** works as a scientist at the FOI Division for Sensor and EW Systems and has a PhD in Applied Physics from the UK. He is project manager of several technology-based projects and studies how modern security technology and surveillance techniques can affect citizens' integrity and privacy. Steven is also an Associate Professor at the Royal Institute of Technology (KTH) in Stockholm.

**Louise Simonsson** holds a PhD in Environmental Analysis. Her research focuses on sustainable security, particularly vulnerability and adaption to environmental and climate changes and environmental threats and risks to society and operations' personnel. This work is done in support of Swedish international operations and medical intelligence. She has mainly worked on Scandinavia, the Arctic and developing countries in Africa, Southeast Asia and Latin America.

**Pontus von Schoenberg** has an MSc in Meteorology and has worked with dispersion modelling and dispersion scenarios since 2002. He has worked with models for simulating dispersion of gases and particles in air, both indoor and outdoor, short-range and long-range. Pontus is involved with the national preparedness for radiological threats in Sweden, in collaboration with the Swedish Meteorological and Hydrological Institute on behalf of Swedish Radiation Safety Authority. He has also given lectures in dispersion meteorology at the NBC Defence Centre for the Swedish Armed Forces and at Umeå University.

**Peter Stenumgaard** has a PhD in Radio Communications and works as Research Director and Adjunct Professor. He leads the research with a focus on interference-resistant radio communications for both military and civilian applications. He is also the Director of the graduate school Forum Securitatis (funded by Vinnova) within Security and Crisis Management. He worked for several years on the JAS fighter aircraft project with the protection of aircraft systems against electromagnetic interference, lightning, nuclear weapon-generated electromagnetic pulses (EMPs) and high-power microwaves (HPMs).

**Magdalena Tham Lindell** is the Cheif Editor of Strategic Outlook 2013 and Team Leader for FOI's Studies in African Security. She focuses on peace building, especially security sector reform and civil and military peace support operations, as well as conflict analysis. She has a Master's degree in Political Science and Peace and Conflict Research from Uppsala University and the Institut d'études politiques in Paris.

**Annica Waleij** is Senior Analyst and Project Manager in FOI's Division for CBRN Defence and Security. She supports the Armed Forces Medical Intelligence with environmental expertise and performs research on environmental and health risks in peace operations. She has trained UN and ECOWAS personnel in e.g. the Democratic Republic of Congo, Ghana, Nigeria and South Sudan. In 2012 she was seconded by the Swedish Civil Contingencies Agency (MSB) to the UN Office for the Coordination of Humanitarian Affairs (OCHA) in Geneva, Switzerland. She has a Bachelor's degree in Environmental and Health Protection and a Master's degree in Environmental Chemistry.

**Misse Wester** is a researcher at the FOI unit for societal safety and security where her research is primarily focused on better understanding and improving risk and crisis management. Misse's main research interest is the perspective of the individual in the contexts of both risk perception and human behaviour during crises. She has a PhD in Psychology and is an Associate Professor in Behavioural Risk Research.

**Mikael Wiklund** is a defence economist and heads an operational analysis group at the Swedish Armed Forces Headquarters. Mikael has previously worked with matters regarding strategic management of the Armed Forces and has served as an expert and later investigation secretary/officer to the Official Reports of the Swedish Government's inquiry concerning defence structures (Försvarsstrukturutredningen). He has an MA in Economics.

**Åke Wiss** has a background as an operations analyst at FOI and currently heads a project offering support to the Swedish Armed Forces' long-term planning. Previously, he has also supported the Swedish Armed Forces with strategic analysis.

The Swedish Defence Research Agency (FOI) is one of Europe's leading research institutes in the defence and security sector. The agency is financed by government appropriations and commissions for specific projects. It reports to the Ministry of Defence. FOI's core activities are research, and technological and methodological development.

FOI first published Strategic Outlook in 2009. It is an annual study on current and future trends in the fields of defence and security, and their strategic implications across a number of geographic and thematic areas.

Strategic Outlook can be accessed from www.foi.se.

FOI

ISSN 1650-1942

www.foi.se