



Strategic Security Analysis

Securing the Future: The Use of Strategic Foresight in the Security Sector

Beat Habegger



Key points

- Modern security policy is shifting from focusing on all types of risks to adapting to all types of situations. Security organisations – defence ministries, intelligence agencies, police forces and armed forces – must therefore increase their focus on resilience-oriented security management.
- Strategic foresight can make an important contribution to resilience-oriented security management because it enables a synchronised focus on multiple threats embedded in a longer-term security perspective. Several security organisations, including NATO, have already begun to use strategic foresight.
- Security organisations should select strategic foresight activities very carefully to ensure they serve their intended purpose. The process model and success factors outlined in this Strategic Security Assessment (SSA) provide guidance on what is needed for making forward-looking thinking and action to become the norm in security policy and security organisations.
- Strategic foresight has the potential to change the way in which organisations and their employees think, behave and act. As such, it can strengthen efforts to prevent, defend against and mitigate security risks, and contribute to the effective security management of the current and future risk landscape.

About the Author

Dr Beat Habegger is an independent advisor on strategic risk management, strategic foresight, and strategic issues in sustainability and public policy. He joined the GCSP as an Executive-in-Residence, Global Fellowship Initiative, in 2021 after more than a decade in various roles at Swiss Re, including Head of Political Risk Management. Previously he worked as a risk and security consultant in a private consulting firm and at the Centre for Security Studies at ETH Zurich. He is a lecturer at the University of St Gallen and a member of the International Advisory Board of the ZHAW School of Management and Law. He holds an MA and PhD from the University of St Gallen.

Introduction

The pace of change has accelerated in all areas of society. Increasing geopolitical tensions, deeper socio-economic divides, rapid technological changes, and the threat of environmental disasters have created the perception that political and economic realities are shifting and society must be reshaped. Organisations of all kinds must respond to these changes and the resulting uncertainties to successfully navigate into the future.

Security organisations – defence ministries, intelligence agencies, police forces or armed forces – are no exception. Like others, they need to improve their capacities to *look ahead* and *think beyond*. The latter is the ability to think beyond system boundaries and to integrate more perspectives into their strategic risk assessments than they were used to in the past. Security organisations must therefore broaden their scope in terms of relevant policy areas far beyond the focus on traditional security issues. On the other hand, to look ahead is the ability to think further into the future than previously seemed necessary. Security organisations must therefore extend the time horizon of their strategic outlook to five, ten or even thirty years to capture all the developments that are potentially relevant to the fulfilment of their mission.

This analysis places strategic foresight at the heart of organisational or management perspectives that help security organisations to meet the challenges they face. By sharpening their strategic foresight, security organisations and professionals can identify significant developments early on and create resilient pictures of possible future environments. This enables them to anticipate threats and opportunities, think and act in terms of alternatives, and optimise their strategic direction and operational management.

Several security organisations have already begun to use strategic foresight. A notable example is NATO's *Strategic Foresight Analysis 2017 Report*, which is designed to help the organisation's leadership to visualise the future security environment.¹ Another example at the country level is the UK Ministry of Defence's report *Global Strategic Trends*, which outlines the future defence and security environment through 2050.² Finally, strategic foresight outputs also address specific issues and developments. The *Human Augmentation project*, for example, a joint initiative between the UK and German armed forces, captures current trends in the world of technology and identifies the implications and lessons for defence.³

This SSA begins by outlining the changing nature of security risks and the need for resilience-oriented security management. It then proposes strategic foresight as an approach that increases resilience by simultaneously “looking ahead” and “thinking beyond”. Next, the various purposes of strategic foresight approaches are outlined to improve decision-making in the prevention of, defence against, and mitigation of risks. Finally, it explains the success factors of strategic foresight in security organisations, followed by some general conclusions.

By sharpening their strategic foresight, security organisations and professionals can identify significant developments early on and create resilient pictures of possible future environments.

Facing the challenge: from risk to resilience in security management

Security policy deals with the prevention of, defence against, and mitigation of risks and threats.⁴ In recent years the understanding of security has changed. Besides the proliferation of actors in the field of security, the scope of security risks has expanded considerably. Security is no longer exclusively a matter of defence against military threats, but now encompasses many other issues such as pandemics, trade conflicts, migration, terrorism and climate change. Many issues are interdependent, and the security dimension is only one of several relevant factors constituting the security landscape. In most cases these issues are global in scale, transnational in their consequences, and cannot be resolved by individual states acting alone. They can only be effectively addressed with combined forces, perseverance and a long-term political vision.

The focus of security policy shifts from protecting against potentially endless varieties of possible risks to how to increase the overall resilience of the state and society.

As in many other areas of business and public policy, the concepts of risk and risk management permeate the security sector.⁵ No organisation – be it a company, a government, an intelligence agency or an army – can identify everything that could go wrong, and it would be unaffordable to prepare for every identified risk. Conversely, it is too risky for any organisation to prepare for only a handful of potential contingencies. In addition, there may be legal duties, political circumstances or moral obligations that require organisations to manage identified risks. In this situation, risk-based practices can help organisations to prioritise risks and weigh the costs and benefits of operational interventions. This is the main reason for the widespread use of risk-based management in business and public policy, including the security sector.

The fact that it is impossible and unaffordable to prepare for every potential risk, even when one is legally, economically, politically or morally obliged to do so, has shifted attention to resilience-oriented management approaches. Resilience is the ability to withstand any shock, regardless of what triggered the shock and its specific impact. Resilience-oriented management therefore focuses less on specific risks and more on “hardening” organisations in a world characterised by both known and unknown risks. Resilient organisations, countries, or individuals are able to cope with what has happened and bounce back quickly and effectively into their pre-shock state, independently of whatever has thrown them off track.

The focus of security policy therefore shifts from protecting against potentially endless varieties of possible risks to how to increase the overall resilience of the state and society. To perform this task, security organisations must adequately address the changing conditions of the risk landscape⁶ and adapt accordingly in terms of how they plan and act to protect against security risks.

Increasing resilience: looking ahead and thinking beyond

The reorientation in security policy from risk to resilience is an indication of the waning confidence in public policy's ability to comprehensively manage the future.⁷ Resilience accepts that disruptions and shocks are inevitable even if everything possible is done to prevent them. The concept of resilience “foregrounds the limits of predictive knowledge and insists on the prevalence of the unexpected”.⁸ The key to managing the future is thus “to learn how to adapt in all kinds of situations” and to act proactively without pretending that the future is already known.⁹

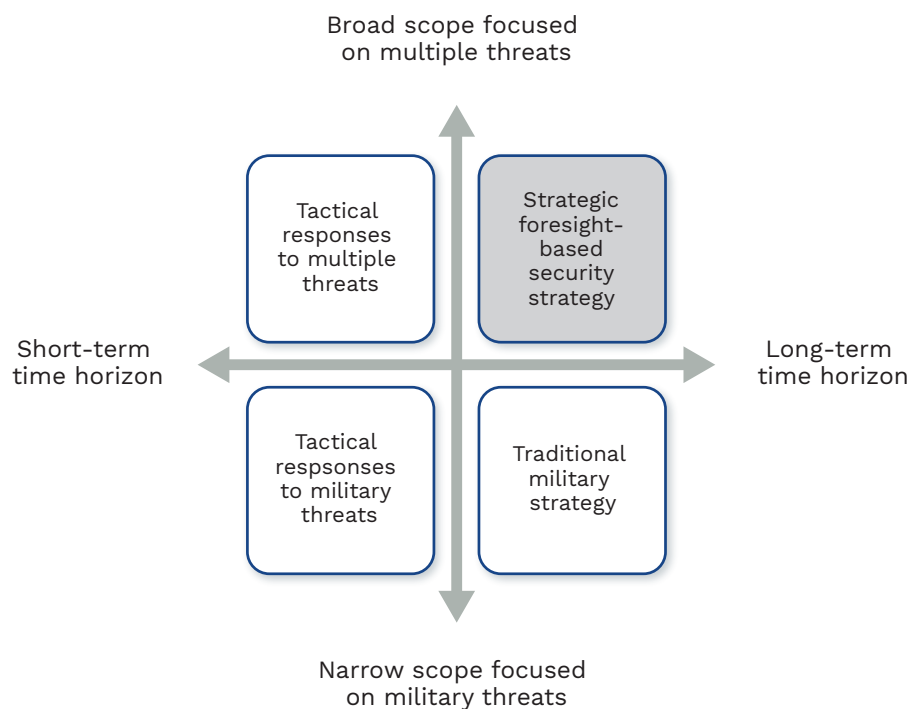
In view of the expanded risk spectrum, the longer time horizon, and the focus on increasing resilience, security organisations must improve their ability to *look ahead* and *think beyond*.

In view of the expanded risk spectrum, the longer time horizon, and the focus on increasing resilience, security organisations must improve their ability to look ahead and think beyond.

- *Think beyond* means that security actors must transcend their traditional system boundaries and integrate more perspectives into their risk assessments than they did in the past. Besides traditional military considerations, this requires them, for instance, to consider security threats associated with technology, biology, cyberspace, artificial intelligence, outer space, natural catastrophes and many more.
- *Look ahead* means that they must think further into the future than seemed necessary in the past. The relevant time frame is now twenty to fifty years rather than two to five years. The strategic outlook is thus expanding to an even longer time horizon.

Figure 1 outlines the options for security management in terms of the two dimensions of scope and time horizon.

Figure 1. Security management in terms of scope and time horizon



The linking of today and tomorrow eliminates the contradiction that while many policymakers are aware of the importance of long-term trends, they are unable to respond to them in their day-to-day work.

- A *short-term time horizon* focuses on tactical responses that are not well embedded in a longer-term vision of the risk landscape. Such an approach is appropriate for emergency responses, but not for strategically focused security management.
- A *narrow scope* follows the traditional security policy path of concentrating on military threats. Although such threats remain important, an exclusive focus on them is no longer appropriate in the context of an expanded risk landscape.
- What is needed instead is a *synchronised focus* on multiple threats (broad scope) embedded in a longer-term outlook on the risk landscape.

A synchronised focus supports security organisations in their attempts to simultaneously look ahead and think beyond – beyond the horizon of conventional system boundaries and with a long-term view of possible future scenarios.

A management perspective that supports the implementation of such a vision is that of strategic foresight. It helps organisations to identify developments at an early stage, create resilient visions of the future, anticipate coming threats, and think and act in terms of alternatives when shaping policy responses.¹⁰ Such a foresight-based approach thus supports security organisations in shifting their orientation from a risk-focused to a resilience-focused security strategy.¹¹

Preparing mitigation strategies: using strategic foresight to strengthen security management

To understand the purpose of strategic foresight, it is helpful to understand the body of knowledge from which it emerges. On the one hand, such foresight draws on *trends research*: its goal is to perceive and interpret social, technological, economic, ecological, cultural, or political events or developments that can influence and shape an organisation's environment. Strategic foresight also draws on *futures research*: its goal is to anticipate future trends and developments in order to envision various possible future situations. The combination of trends and futures research not only leads to a comprehensive view of the current risk landscape, but also enables the development of ideas about how this landscape will develop in the future. This linking of today and tomorrow eliminates the contradiction that while many policymakers are aware of the importance of long-term trends, they are unable to respond to them in their day-to-day work.

In the security context, strategic foresight thus means integrating trends and futures research with the aim of providing security organisations with the basis for plans and policies to prevent, defend against and mitigate risks. Three strategic foresight approaches can be distinguished:¹²

- Strategic foresight can pursue an *exploratory purpose* and follow an analytical logic. In this case, it focuses on an improved understanding of an organisation's external environment. It emphasises observable trends and seeks to capture early warnings and weak signals that help to anticipate likely futures.
- Strategic foresight can be understood as a *learning process*. In this case, the focus is often on scenario development. The goal is to identify potential risks against the backdrop of a range of possible future

Foresight must be directed towards impacting an organisation at the institutional, procedural, or managerial level, and aim at triggering changes in terms of policy decisions and priorities.

scenarios and to draw the necessary conclusions for the political and institutional orientation of the actors or organisations involved.

- Strategic foresight can have a *normative purpose* by creating a shared vision of the future that is consistent with an organisation's preferences. The goal is to create shared commitments to strengthen future orientation, support team building, enable cultural change and transform the organisation in a desired way.

These three approaches are not mutually exclusive and can be combined to take advantage of their respective strengths. In the public sector, including the security sector, the focus is usually on the first two approaches, i.e. exploratory and learning-oriented strategic foresight. Taking a long-term perspective and thinking in terms of a range of possible scenarios are familiar to many security professionals when, for example, they are preparing to deploy forces or making investment decisions to acquire force equipment. Security organisations can therefore draw on this wealth of experience and embed strategic foresight in their security management processes.

Implementing strategic foresight in the security sector: processes and success factors

The strategic foresight approaches described above follow a similar pattern in their process logic, especially when they combine an exploratory and a learning-oriented approach.

- In a first step, relevant environmental information is collected, processed, analysed and evaluated. The aim must be to cover as broad a spectrum of possible developments as possible – political, economic, social, technological, cultural, environmental, or whatever else is considered to be relevant – while linking the current situation with these possible future developments.
- The second step is to design future projections. This often takes the form of a scenario-based approach. The scenarios that are developed are then transferred to the context of a country or security organisation in order to derive the most important lessons.
- In a third step, the risk landscape and the possible consequences resulting from future scenarios are then translated into strategy-relevant conclusions. These can then form the basis of new or adapted policy responses and the necessary adjustments that security organisations will need to make in terms of their mandate, structure, processes or leadership.

The last step is crucial, because the processes described above should never constitute an end in itself. Strategic foresight projects must trigger effects if they are to be of practical relevance: if there is no will to change, strategic foresight is pointless. In practice, this means that such foresight must be directed towards impacting an organisation at the institutional, procedural, or managerial level, and aim at triggering changes in terms of policy decisions and priorities.

Most strategic foresight activities share common characteristics.¹³ Analysing them reveals information about the success factors of strategic foresight, but also about whether and to what extent organisations are challenged by these activities. This is especially the case when such activities question or even contradict the routines, traditions, or cultural

Foresight requires a systematic effort that spans the entire organisation and involves changing the way in which people think and act.

self-images of organisations and their employees. The extent to which this is relevant depends on the context of strategic foresight projects. Are they in the public or private sector? In which industry sector or policy areas are they being used? Is the focus on technology policy, social policy, environmental policy or security policy? Depending on this, different requirements will apply to specific types of organisations and their employees.

In the following discussion, therefore, the success factors of strategic foresight specifically apply to the area of security and defence policy.

- *Strategic foresight is a process, not a (forecasting) technique.* The point is that strategic foresight is not about predicting the future by forecasting developments or trajectories; consequently, it is more than simply applying a particular method taken from a methodological toolbox.¹⁴ Rather, it requires a systematic effort that spans the entire organisation and involves changing the way in which people think and act. Because of the transformative potential of strategic foresight, it is essential that an organisation's leadership fully supports such projects and initiatives, even in the face of internal and external resistance.
- *Strategic foresight is a participatory approach.* Strategic foresight cannot be delivered in command-and-control mode. It requires a broad spectrum of people from various corners of an organisation and a modern understanding of leadership that goes beyond the traditional top-down model. Security organisations – especially armed forces or police forces – are hierarchically organised and are permeated by a corresponding organisational culture. However, the success of participatory approaches depends on the ability of leaders to overcome hierarchical boundaries so that people from all levels of the organisation are comfortable to freely share their views and thoughts in strategic foresight projects.
- *Strategic foresight is an interdisciplinary endeavour.* An important reason for introducing strategic foresight into the security domain is the need to incorporate additional perspectives than the traditional focus on military considerations. This requires the involvement of people with multidisciplinary expertise from a wide range of professional experiences and academic backgrounds. If security organisations are unable to recruit such people internally, they should consider ways to create this diversity through the targeted involvement of individuals from outside the organisation.
- *Strategic foresight requires a diversity of views and insights.* Strategic foresight requires creativity and a certain amount of unconventional thinking in order to imagine possible futures that are very different from what can be observed today. However, organisations in all sectors tend to hire similar groups of people with shared characteristics and backgrounds. To some degree, this is inevitable. An organisation may indeed need employees with a particular background (e.g. engineers, financial experts, legal advisers, etc.) to successfully accomplish its mission. And the employees will have each chosen to devote their time and resources to the cause championed by that organisation. In any organisation, “groupthink” – i.e. when co-workers start thinking alike or very similarly – is a menace that negatively impacts creativity and innovation. Security organisations are particularly vulnerable to a lack of diversity in terms of gender, ethnic background, and – to some extent – professional and academic profiles.¹⁵ Therefore, as mentioned before, the solution is to supplement in-house staff with externally recruited people to achieve a more pluralistic mix in strategic foresight activities.

Although there is commitment to the long term in many organisations, the focus nevertheless quickly turns to short-term fixes when the next crisis hits.

- *Strategic foresight takes a long-term perspective.* Since strategic foresight is based on futures research and aims to look further into the future than traditional planning approaches, a longer time horizon is inherent to this process. Although there is commitment to the long term in many organisations, the focus nevertheless quickly turns to short-term fixes when the next crisis hits. The expectations of policymakers and the public reinforce this tendency. In such situations, strong leadership is needed to defend an organisation's long-term focus and not lose sight of longer-lasting trends and developments in the storm of crisis.
- *Strategic foresight must be decision-oriented, without providing ready-made strategies.* The acceptance of strategic foresight depends on whether it leads to effective and sustainable management solutions. It is subject to prejudices, such as that it is merely a kind of crystal-ball gazing and lacks analytical rigour. These views have the potential to undermine the credibility of strategic foresight activities; indeed, they can be used strategically by those who want to preserve the status quo and prevent an organisation from effectively repositioning itself in a changing environment. Thus, the acceptance and continued success of strategic foresight requires that it has a positive impact on security organisations. It must help leaders to develop better strategies, better policies, better organisational practices, better investment decisions and better leadership.

These characteristics and success factors clarify that strategic foresight is not just about applying a particular method from a particular methodological toolbox.¹⁶ Rather, it is about integrating future-oriented thinking and action into entire organisations. This is why strategic foresight is also associated with a transformative promise: it fosters the ability to step out of entrenched mindsets and practices, and it transforms participation and decision-making processes so that organisations begin to act and behave differently and more effectively.

Conclusions for the security sector

1. Strategic foresight is a central component of a resilience-oriented security strategy.

Modern security policy is shifting from *focusing* on all types of risks to *adapting* to all types of situations. Meeting future challenges requires forward-looking action, but without claiming to be able to predict everything. In other words, security organisations need to increase their focus on resilience-oriented security management. Strategic foresight can make an important contribution to this endeavour. The perspective of *thinking beyond* and *looking ahead* forms the basis of a such a strategy, because it enables a synchronised focus on multiple threats embedded in a longer-term security perspective.

2. Strategic foresight improves organisational security management capabilities.

Strategic foresight serves different purposes, and every security organisation needs to think about its own intended purpose: exploratory, learning-oriented, or normative goals can all contribute to a foresight-oriented security strategy. The ultimate choice – including the combination of different approaches – depends solely on the intended outcomes. In summary, strategic foresight unleashes creativity in organisations; is guided by the need for deeper insights and understandings; improves the quality of organisational action and decision-making; and supports change at the organisational and individual levels.

3. Strategic foresight can be effectively implemented in security organisations.

Strategic foresight has the potential to transform the way in which organisations and employees think, behave and act. Because such foresight focuses on (uncertain) futures, a certain methodological rigour is required. The process model and success factors discussed above provide guidance on what is needed to make future-focused thinking and action the norm, rather than the exception, in security policy in particular and public policy in general. In this way, strategic foresight strengthens security organisations' efforts to prevent, defend against, and mitigate security risks, and thus contributes to an effective security management of the contemporary and future risk landscape.

Strategic foresight is a central component of a resilience-oriented security strategy.

Endnotes

1. NATO (North Atlantic Treaty Organisation), *Strategic Foresight Analysis 2017 Report*, November 2017, https://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf.
2. UK MoD (Ministry of Defence), *Global Strategic Trends: The Future Starts Today*, 2 October 2018, <https://www.gov.uk/government/publications/global-strategic-trends>.
3. Future Analysis Unit, *Human Augmentation: The Connection between Man and Machine*, 17 May 2021, <https://www.bundeswehr.de/de/organisation/weitere-bmvg-dienststellen/planungsamt-der-bundeswehr/-human-augmentation-verbundung-mensch-maschine-planungsamt-5016384>.
4. The concept of risk assumes that a hazard encounters a vulnerable system. For example, an avalanche is a hazard, but it becomes a risk only when it affects an inhabited or populated area. In general, risks are characterised by the fact that (a) they occur in the future; (b) the specific future event is uncertain; and (c) people can act and thus influence the outcome of a future event. Risks are referred to as “calculated uncertainty” (Frank Knight), because the probability of an event (hazard) occurring is associated with the magnitude of the damage (to the vulnerable system). Fundamentally, risk is neutral in the sense that it can represent both a threat (with downside potential) and an opportunity (with upside potential). Because the threat aspect usually predominates over the opportunity aspect in security policy, the terms “risk” and “threat” are often used interchangeably, although this can be conceptually misleading.
5. B. Habegger, “Von der Sicherheits- zur Risikopolitik: Eine konzeptionelle Analyse für die Schweiz”, in A. Wenger (ed.), *Bulletin 2006 zur schweizerischen Sicherheitspolitik*, Zurich, Centre for Security Studies, ETH Zurich, 2006, pp.133-164.
6. The risk landscape is the result of cognitive models of individuals or groups, with the help of which they conceptualise the threats and opportunities in the world. These models are essentially based on individuals’ and groups’ experiences, interests and values. See M. Kamppinen and M. Wilenius, “Risk Landscapes in the Era of Transition”, *Futures*, Vol.33(3), 2001, pp.307-317.
7. M. Dunn Cavelty, “From Predicting to Forecasting: Uncertainties, Scenarios, and Their (Un-)Intended Side Effects”, in A. Wenger et al. (eds), *Governing and Probing the Future: The Politics and Science of Prevision*, London and New York, Routledge, 2020, pp.99f.
8. J. Walker and M. Cooper, “Genealogies of Resilience: From Systems Ecology to the Political Economy of Crisis Adaptation”, *Security Dialogue*, Vol.42(2), 2011, p.147.
9. Dunn Cavelty, 2020, p.99.
10. For an overview and extended conceptualisation of strategic foresight, see A.W. Müller, *Strategic Foresight: Prozesse strategischer Trend- und Zukunftsforschung in Unternehmen*, dissertation, University of St Gallen, 2008; see also R.A. Slaughter, *The Foresight Principle: Cultural Recovery in the 21st Century*, Westport, Praeger, 2005.
11. For an application of strategic foresight to public policy, see, for example, A. Leigh, “Thinking Ahead: Strategic Foresight and Government”, *Australian Journal of Public Administration*, Vol.62(2), 2003, pp.3-10; for a comparative perspective, see B. Habegger, “Strategic Foresight in Public Policy: Reviewing the Experiences of the UK, Singapore, and the Netherlands”, *Futures*, Vol.42(1), 2010, pp.49-58; and for an attempt to integrate foresight into security planning and risk management and the intersection of foresight and risk management, see S. Haugdal Jore et al., “The Contribution of Foresight to Improve Long-term Security Planning”, *Foresight*, Vol.20(1), 2018, pp.68-83.
12. Müller, 2008, pp.42-45; K.M. Weber, “Foresight and Adaptive Planning as Complementary Elements in Anticipatory Policy-making: A Conceptual and Methodological Approach”, in J.-P. Voss et al. (eds), *Reflexive Governance for Sustainable Development*, Cheltenham, Edward Elgar, 2006, pp.189-221.
13. Müller, 2008, p.21.
14. It is important to differentiate between foresight and forecasting: while forecasters make probability judgements about events that can be checked against the unfolding reality when they (do or do not) happen, people exercising foresight create plausible scenarios of conceivable (mid- to long-term) developments; cf. L. Brozus, “(Not) Lost in Foresight: Structuring Futures Complexity in a Politically Meaningful Way”, *SWP Comment No. 33*, Berlin, German Institute for International and Security Affairs, 2021.
15. In addition, many security organisations offer – and expect – a lifetime commitment. As a result, staff turnover is low, and staff renewal only occurs through the entry of younger employees into the profession.
16. Various methods and instruments are used in strategic foresight. The optimal choice of such methods and instruments depends on the specific needs and objectives of strategic foresight activities. For a practice-oriented overview, see K. Kohler, *Strategic Foresight: Knowledge, Tools, and Methods for the Future*, Zurich, Centre for Security Studies, 2021, pp.14-15; A. Wilkinson, *Strategic Foresight Primer*, Brussels, European Political Strategy Centre, 2017, pp.13ff.; or UNDP Global Centre for Public Service Excellence, *Foresight: The Manual*, Singapore, 2015.



GCSP

Geneva Centre for
Security Policy

Where knowledge meets experience

The GCSP Strategic Security Analysis series are short papers that address a current security issue. They provide background information about the theme, identify the main issues and challenges, and propose policy recommendations.

Geneva Centre for Security Policy - GCSP

Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
CH - 1211 Geneva 1
Tel: + 41 22 730 96 00
Fax: + 41 22 730 96 49
e-mail: info@gcsp.ch
www.gcsp.ch

ISBN: 978-2-88947-309-0

The opinions and views expressed in this document do not necessarily reflect the position of the Swiss authorities or the Geneva Centre for Security Policy.