The
Federal Government

Strategy Paper of the Federal Government on Strengthening the Civil Security Industry in Germany

Berlin, 21th December 2016

Structure

I. Current domestic and security policy and the need for Germany to have a high-performing civil security industry that is able to compete

With an increasing number of serious crises in the world, several countries neighbouring the European Union becoming more fragile, and with all the major implications of globalisation and technical progress, Germany is facing major challenges in terms of its foreign and security policy. The number of possible threats is growing, as is their intensity. At the same time, Germany's membership of the European Union and its involvement in the transatlantic alliance means that a number of our challenges can only be addressed if we work closely with our European and allied partners.

Government institutions, particularly the public authorities and organisations working in sensitive fields, the private sector and private households must all continuously adjust themselves to a security situation that keeps changing. This also means that German authorities need to be equipped to fulfil their duties. They need modern equipment that reflects the latest state-of-the-art and that lends itself to cross-border and pan-European cooperation, thanks to being highly compatible with other systems, reliable, and consistent. It is particularly important for Germany to become more independent of foreign suppliers of products used to protect confidential facts, items, or intelligence (any form and type of classified information) or any other type of sensitive information, and to use high-quality products manufactured by German security firms instead.

Security and the structures underlying it must be designed in a way that takes into account the universal presence of information and communications technology in all areas, from the public administration, to businesses, and to our private lives. The primary goal of any security system must be to detect and deter potential threats at an early stage. This is why "security by design" ought to be standard practice in the security industry. As we become increasingly dependent on technical applications for our security, we need to ensure that security products meet the highest quality standards and – at least where a high level of protection is required – proven security standards. It is for our national civil security industry to deliver on this.

The Federal Government wants to make use of innovations allowing it to successfully address new challenges as they arise and is therefore willing to engage in a strategic partnership with the civil security industry. As Germany and the European Union seek to gain greater sovereignty in terms of strategy and greater scope for action, they need to be able to increasingly rely on security technology made in Germany or elsewhere in Europe.

Germany is willing to do its bit when it comes to establishing a home-grown, competitive and high-performing security industry in Europe that will help Europe follow a security policy that lives up to Member States' shared responsibility. In its Coalition Agreement, the Federal Government made it very clear that it considers the security industry to be a matter of national interest in terms of the government's economic, technology and security policies. The agreement also sets out the aim of retaining key enabling technologies and jobs in the security industry, and of enhancing the relevant technologies and capabilities.

II. The civil security industry in Germany – its present situation and prospects for the future

1. The civil security industry in Germany

Germany has a strong civil-security landscape with capable companies and research institutes covering the entire value chain, from research and innovation, to components, and to complex systems integration.

What is still missing is a uniform and universally recognised definition of what belongs to the civil security industry in Germany. Products, technologies and services that are developed or deployed for specific purposes related to security feature only partially in the national statistics on security goods. In the interest of having a workable definition of what is the civil security industry, it makes sense to use a functional approach and include all companies that develop and/or sell products, technologies or technical services designed to deliver civil security capabilities.

Products, technologies and services designed by the civil security industry are primarily used to protect critical infrastructure, cyberspace, the airspace and space, the sea, borders, urban space and major public events, to combat terrorism, serious and organised crime, industrial espionage and various forms of extremism, and to respond to natural disasters, pandemics and technical disasters. Government also relies on a large number of products made by the civil security industry for protecting confidential and classified information. The product range of the security industry can be broadly divided into the fields of security technology, security services and IT security. There is, however, a trend towards greater convergence of these.

The civil security industry in Germany is very heterogeneous in terms of the products and services on offer, and also in terms of corporate structures. Many of the SMEs working in this field do a great deal of R&D and are innovative and flexible. They and their highly skilled staff are crucial for the success and competitiveness of the German civil security industry. It is also true, however, that there is still room for more innovations to be translated into marketable products and security solutions. When it comes to the supply of technical components, in particular, the German civil security industry is highly dependent on non-European suppliers and sometimes has a strong focus on finishing and enhancing existing products. There is a lack of experts and skilled labour affecting the various sub-industries to different degrees.

Another point to consider is the fact that the market for civil security solutions is a special one, on account of the role played by government. More than other markets, the civil security industry is affected by the national interest, legislative action, and by government procurement. In many cases, demand stems directly from legislative action (e.g. legal requirements concerning the protection of critical infrastructure or of the electronic data transmission structure for healthcare). The state is responsible for maintaining public order and guaranteeing public security, which makes it a key customer for the civil security industry.

2. Opportunities and challenges

To strengthen the civil security industry in Germany is to create new opportunities for business in Germany. Civil security firms in Germany are part of a highly developed, innovative research and technology landscape. The civil security industry is a sector that has boasted higher-than-average growth rates and is set to continue to do so. Civil security is a priority for Germany and has been declared one of the most important fields of action in the Federal Government's High Tech Strategy of August 2014. Products and services designed around security technology are important not only for our domestic market: given Germany's reputation for being a secure state that ensures freedom, the sector has every possibility to build a specific German "brand" that is successful on the international markets. It is up to industry itself to develop and market products that meet the highest standards of security.

This is happening in a situation whereby threats are becoming increasingly complex and difficult for the civil security industry to deal with, not least given that all aspects of our lives are becoming digitised. Requirements for networked security are set to rise, in terms of technology, manpower, and organisational structures. Where there used to be a clear, physical separation between companies, government institutions and private households, devices and processes are now being joined up to become part of the Internet of Things. This leaves us significantly more vulnerable to attacks from cyberspace (e.g. in the context of Industrie 4.0, automated and networked driving, smart living etc.). Systemic solutions such as security-by-design and privacy-by-design are key to ensuring that digital systems are available, intact, and that the data entrusted to them is kept secure. Digitisation and informational security must be approached as two fields that are intertwined. This will only be possible if there are enough IT experts available.

Given the increasingly complex nature of the threats faced, it is essential that the German civil security industry is capable of delivering systems integration and of assuming a leadership role in this. These capabilities must be safeguarded, expanded and, in some cases, restored. Where needed, this ought to happen in a European context. Only when there are German systems providers in the security sector will it be possible for partial solutions developed by other German and European suppliers to be integrated. The objective here is to combine security technology, security services and IT security to create complete security solutions that are as universal as possible so that they can be scaled up. It is vital to identify those technological fields in which Germany and Europe must regain development and manufacturing capabilities and reduce their dependency on foreign suppliers.

Persistent barriers to entering the European and non-European security markets have resulted in persistent fragmentation of the global civil security market, which in turn is making it very difficult for the German civil security industry to do business internationally.

III. It is against this backdrop that the Federal Government has adopted the following ten-point programme for strengthening the civil security industry, (subject to the relevant figures in the Federal Budget and the Financial Plan):

1. Promoting research, development and innovation

The Federal Government is already promoting research, development, and innovation within the field of civil security. Individual ministries focus on different aspects of this and are involved in this work to different degrees. The Research for Civil Security programme and the Self-determination and Security in a Digital World programme for IT security, which are both being conducted under the leadership of the Federal Ministry of Education and Research, create important momentum for applied basic research in the field of security. The Federal Ministry for Economic Affairs and Energy is providing funding for innovative security technology as part of its Central Innovation Programme for SMEs (ZIM) and its collective research programme (IGF), which are both technology-neutral. Beyond this, the various ministries coordinate on their research programmes to ensure that the right projects are given priority, that any funding gaps are closed, and that security interests are taken into account in the context of other research programmes as well. Other federal institutions that are tasked with research and development also provide valuable support for research, development and innovation in the field of civil security.

The Federal Government will therefore focus its efforts in this field on

- action that helps to close the gap between the prototype-stage and the marketable product (so-called “death valley” for research funding). The aim here is to ensure that a greater number of innovations break onto the market. One of the ways of achieving this can be to encourage greater and smarter involvement of the end users of civil security technology in the process of product development. This must be done without deterring end users who may be afraid that they will be left with product developments that are not quite ready for market.

- assessing the possibility of initiating ground-breaking research pilot projects with the intention of rolling these out across the country, which also means assessing ways in which support can be given during the stage of product testing up to the product’s entry onto the market – without violating the ban on using public-sector research funding to support the final stages of development of prototypes. Given the limited volume of the market and the difficulty of predicting the outcome of public procurement procedures, industrial partners have so far shied away from the risk of investing in the final development stages of innovative security solutions that already exist in prototype and have the potential to become marketable products.

- assessing how standards can be developed parallel to the product development, which will allow for products to pass conformity assessment tests, and how the necessary legal environment can be put in place/adjusted in time.

- assessing if and to what extent it makes sense to raise overall protection levels for information and communications technology by providing funding for security solutions which can be rolled out for free or in return for a small fee, but whose deployment would not be economically viable without this funding. This would also require an assessment as to whether the relevant case is a one of specific market failure or whether the business environment needs adapting.

- using any scope that exists for reducing red tape around funding for research, development, and innovation.

- working with the German states to see whether there is potential for imparting better IT security skills in schools, universities, in vocational training, and in continuing education.

- taking into account that it will often not be possible for the investments associated with product development to pay off if the product is only sold on the German market. A reliable business environment is needed so that it is possible to arrive at a realistic estimate of the size of the market, and of the volume of potential exports. It is also a fact that high certification standards for products and services that also afford adequate protection of classified government information and a high level of data privacy that is in line with the needs of the market represent a competitive advantage for the German security industry, one the sector can build on further.

2. Breaking into markets abroad

Supporting the German civil security industry in its efforts to do business abroad is a task that must be completed in recognition of the fact that the companies forming this industry tend to be SMEs with a strong focus on their regional and domestic market, and that foreign security markets tend to be difficult to access. Internationally, these markets are dominated by public-sector buyers, they are heavily regulated and, because they are closely linked to the issue of sovereignty, they are seen as a sensitive area. In many countries abroad, the public sector is in charge not only of matters that are traditionally considered to fall within the scope of homeland security (police, civil protection, fire brigade) and acts as a buyer of security solutions for these applications, but also of some types of critical infrastructure. Furthermore, requirements for security solutions differ from country to country and thus create barriers to market entry that indirectly have a protectionist effect. For all these reasons, it is almost impossible for firms working in the civil security sector to gain access to decision-makers in government without having political backing. Procurement practices and the structure of the customer base mean that companies wishing to do business and form networks on non-European markets are dependent on political support. The Federal Ministry for Economic Affairs and Energy and its export initiative for Civil Security Technology and Services play a very important role here.

Whether or not a company is able to win a contract for a large-scale project abroad will often depend on its ability to offer systems leadership and systems integration. Security systems providers also fulfil the important task of acting as door-openers for SMEs working in the industry. When designing instruments to support systems leaders in exporting their products and services, the Federal Government must take account of the fact that the risk incurred by these companies goes beyond the usual business risk.

The Federal Government ought to follow a holistic approach that systematically integrates its industrial policy into its wider security and development policies and any related initiatives. Cooperation within the security industry could become an important part of new strategic partnerships on security.

The government's policy on export controls for dual-use goods has a major impact on the German civil security industry and its foreign business. Additional harmonisation is required within the European Union – not least as far as administrative practice is concerned – so as to level out the European playing field. Furthermore, a streamlining of licensing procedures is of the essence for exporters. This is particularly acute where information and communications technology is concerned – an industry that is characterised by very short product cycles. Whether or not a company is able to win a contract will often depend on how it takes for the export licence to be issued. Long delivery periods are particularly harmful where spare parts and services are concerned. Contracts will usually go to companies that are able to guarantee that they will immediately conduct remote assessments and repair work and deliver spare parts promptly.

This is why the Federal Government will notably

- look into ways of further optimising its instruments to promote foreign trade and investments.

- look at ways in which the German civil security industry could better position itself to win contracts for major international events (e.g. FIFA World Cup, Olympic summer and winter games), not least by working with the bilateral chambers of industry and commerce and with Germany's representations abroad.

- make it standard practice to look at possible ways in which the German civil security industry can become involved in any bilateral development cooperation work undertaken by the Federal Government and which extends to security matters; this will be done in compliance with implementing agencies' need to be neutral under competition law, and abiding by the principle of untied aid.

- seek to process applications quickly and further optimise the relevant procedures. Licences issued for a first delivery should serve as guidance for additional deliveries at a later point.

3. Optimising public procurement

The public sector continues to be one of the most important domestic customers for the German civil security industry. There is a need for the various procurement agencies that exist at all levels of government within the Federal Republic of Germany (federal, state, municipal) and that act autonomously to better coordinate on their demand. This would leave the various security and rescue forces in a better position in terms of their interoperability and would also create economies of scale within the civil security industry. Furthermore, public-sector demand for products manufactured by the civil security industry also has an impact on the German and European security industries' ability to compete at global level.

There are cases in which public-sector procurement agencies may not be aware of the existence of new, innovative security solutions. This means that the full potential for public procurement to promote innovation is not always used. Also in this context, it is important to ensure that any interfaces that can be used to link up various security solutions ought to be designed to be as open as possible. Public procurement could play a stronger role when it comes to promoting innovation. This could notably be achieved by improving communication between the supply and the demand side, by making better use of instruments such as contracting at the pre-competitive stage, public-private partnerships, and pre-competitive dialogue.

The Federal Government is aware of the fact that foreign customers seeking to purchase German security technology will often look to Germany's public procurement agencies as a reference, meaning that procurement decisions taken at national level may have a major impact on a company's ability to secure contracts internationally.

The Federal Government will notably examine whether

- it makes sense to establish a platform for dialogue / a database which could be accessed by all procurement agencies within the country, allowing them to thoroughly assess and compare the products that are available.

- it is possible to use procurement procedures for state-of-the-art security technology to give a boost to demand for innovative products.

- it is possible to increase the extent to which the neutral expertise of research and science institutes is drawn on in public procurement procedures. One way of achieving this could be to establish dedicated centres of excellence that would offer consultancy services to public-sector customers.

4. Harmonising standards and certification schemes

The existence of different standards and certifying procedures within and beyond Europe represents a major non-technical barrier to trade and comes at a high cost for companies. This makes it necessary to strive for greater transparency and better harmonisation at European and international level. Equivalent standards and certifying procedures would allow for economies of scale and greater competition – without compromising the high standards of security that apply in Germany. Coordination on national standardisation processes from an early stage and placing a focus on areas that are strategically important will allow for standardisation to be successfully used as a tool that can open up markets for the German security industry. German companies and authorities ought to seek to be actively involved in European and international standardisation processes so that they can continue to set global trends with

their innovative products and services. The NIS Directive on security of network and information systems and the need for certification of data processing tools under the General Data Protection Regulation provide for good opportunities for this. It is for the private sector to take the initiative on such activities. Government's role in this is to support and – if necessary – adjust these processes, for instance by being represented within the relevant standardisation bodies.

Requirements for certification are high in Germany, a fact that the German civil security industry can use to its advantage as it advertises "security made in Germany". By the same token, these high benchmarks serve to prevent the use of product components that are less insecure or less trustworthy.

The Federal Government will therefore

- ensure, to the extent that this falls into its scope of responsibility, representation of small and medium-sized companies in national and international standardisation bodies and advocate for standardisation processes to be conducted at European and/or international level.

- advocate greater use of "localised" international standards in all cases other than those where only national standards that go beyond what has been agreed at international levels can ensure that overriding national security interests are served.

- expand Germany's assessment capacities capable of dealing with higher levels of protection.

- promote integration of conformity-assessment programmes into European and international accreditation schemes.

- consolidate and prioritise its certification activities and assess whether introducing separate quality hallmarks for different security standards could help build greater trust in security products and product security on the part of private households, companies and within the public sector.

5. Creating clusters

Just like in other industries, close networking between the relevant stakeholders in the civil security industry is a key factor that fosters innovation and a rapid translation of new findings into marketable products. Most of all, it is key that the end users of the products and services are closely involved, as this is the only way in which companies will be able to tailor their solutions to customers ever more specialised needs. Strong clusters that cover the entire value chain from research to the final product can evolve into core structures for the development of innovative security solutions and serve as reference projects for future exports. At the same time well-functioning cluster structures can also act as multipliers that ensure that SMEs, in particular, also benefit from measures to promote external trade and are involved in standardisation work. Clusters, together with better marketing of flagship projects in particular, can help raise the profile of the German civil security industry and testify of its prowess. Moreover, security is another area in which university training ought to be more closely linked up to the programmes designed to support young entrepreneurs and for which dedicated start-up incubators ought to be established.

The Federal Government will therefore

- take more targeted action to promote close cooperation within science, development and manufacturing and to encourage the formation of security clusters. This will be achieved by creating networks bringing together security firms, research and science institutes, and the end users of civil security technology. As it addresses this task, the Federal Government recognises that the Federal Ministry for Economic Affairs and Energy and its "go cluster" programme and the Federal Ministry for Education and Research with its various activities to promote the formation of clusters are already doing a great deal to encourage networking within innovation clusters. Representatives working in the field of civil security are also actively and successfully involved in these programmes.

6. Drawing on the combined expertise of the civil security and defence industries

The emergence of hybrid threats has meant that what used to be a clear line separating homeland security and security abroad is now blurred. This has resulted in the domestic security forces and the armed forces now relying on similar capabilities, at least in some areas. It has therefore become difficult to cleanly separate security technology from defence technology. Technologies that are used for security and defence purposes alike include cyber security solutions, protection against chemical, biological, radiological, nuclear and explosive substances (CBRNE) and against autonomous unmanned systems, protective clothing, sensors and sensor data fusion technology, situation awareness and analysis technology, among many others.

This means that much is to be gained from systematically pooling the knowledge, know-how and experience gained within the civil security and the defence sectors. Synergies of this kind are already being used as companies and institutes from the defence sector are involved in research and development work for civil technology. In addition to this, a new programme for innovation called "supporting defence companies as they seek to branch out into civil security technology" provides incentives for greater cooperation between companies working in the defence industry and in civil security.

Closer contact between the German armed forces (Bundeswehr) and the Federal and state security agencies could also be used to transfer expertise and exchange experiences between the security and the defence industries. The civil security industry would notably benefit from information shared by the defence industry about its experiences placing systems offers on the international market.

The Federal Government will therefore

- initiate open dialogue, without any preconceived answers, with the states, with research and science institutes and with universities, on a potential use of civil clauses.

- revisit the issue of civil clauses in banking, which currently prevent financing from being granted for dual-use technologies; this is in response to the changed security situation which is increasingly defined by hybrid challenges.

7. Defining key enabling technologies

Defining national key enabling security technologies and maintaining these in Germany serves to uphold Germany's strategic sovereignty in the field of security policy. This includes the capability to guarantee a reliable supply of our security forces and to independently maintain critical infrastructure in working condition.

Key enabling security technologies notably include technologies that we need to build a digital economy and society and keep these secure. This applies to basic and manufacturing technology for network technology, microelectronics, cryptographic processes, cloud-based memory systems and technologies used to make IT systems more resilient.

The Federal Government will therefore

- work to retain key enabling security technologies in Germany by prioritising research and development funding for these areas across government, by taking procurement decisions accordingly, by deploying its instruments designed to promote foreign trade and investment, and by means of targeted industrial policy. This will also include an assessment as to whether foreign investment control can be extended so as to protect companies that are in possession of crucial expertise (particularly SMEs) from being taken over by non-European investors.

- strengthen microelectronics, which is a crucial technology underlying not least security applications used within the digital economy and Industrie 4.0. A sum of one billion euros has already been earmarked for this purpose within the budget of the Federal Ministry for Economic Affairs and Energy for the 2017 to 2020 period, as part of an important project of common European interest (IPCEI).

- conduct an assessment as to whether additional legal adjustments of the fiscal framework and/or new lighthouse projects are a promising means of strengthening key enabling technologies.

- promote cooperation between systems suppliers (over-the-top suppliers) / global players and the German security industry and IT security industry; subject to certain requirements, the government will also demand that such cooperation take place.

- look into the possibility of establishing a dialogue platform for trusted information technology, which would create the added benefit of bringing together the expertise of the German IT security industry and of the manufacturing industry.

- look into ways of improving or finding alternative ways of creating the statistical database from which the key economic parameters of the civil security industry are derived (sales, employment, growth); a database which has so far been less than solid.

8. Supporting SMEs

German SMEs act as a driver of innovation within the German economy, create jobs and deliver training. The German security industry is dominated by small and medium-sized companies. This means that any action to support SMEs in Germany will also benefit the German civil security industry as a whole. One key objective here must be to encourage greater networking within the security industry, which continues to be very fragmented. Systematic cooperation between German SMEs providing highly specialised security technology and large German systems providers that cater to the global markets is likely to make the German security industry more competitive internationally.

SMEs working in the security sector rely on administrative procedures to be straightforward. This means that application and licencing procedures ought to be streamlined to the greatest possible degree.

The government will consider whether there is a need for additional instruments promoting foreign trade and investment to be introduced, which would cater to the needs of SMEs and exist alongside the export initiative for civil security technology and services. For instance, it would be possible to directly support companies in selling their products and services to growth regions. Support for German systems providers wishing to secure contracts for major international projects might be given subject to a national content quota being met – a requirement that would benefit small and medium-sized firms.

The Federal Government will therefore

- improve civil security firms' access to financing and venture capital. Whether or not a company is to be granted a loan is to be decided in recognition of the fact that civil security companies' ability to generate sales is dependent on government export control.

- look into ways in which it can support small and medium-sized companies in their efforts to sell their products and services internationally.

9. Improving the European framework for the civil security industry

The European civil security market continues to be very fragmented. There are barriers to trade that prevent companies from being able to compete on a level playing field and generate economies of scale.

Uniform standards and certification procedures that do not go below German security levels are a key factor for companies to be able to scale up their business and for European security solutions to become more successful on the international markets. The relevant European technology platforms can help to advance the work towards better harmonisation. Public-sector funding for research and development in the field of civil security, most importantly the

funding provided under the security chapter of the European Research Framework Programme, helps pool the technical security expertise that is available in Europe and create pan-European security clusters. As is the case at national level, synergies between the security and defence industries ought to be created at European level as well. When it comes to strengthening the single market and levelling out the playing field within Europe, greater harmonisation of procurement law and administrative practice is needed, as is greater convergence on export control where dual-use goods are concerned. It might also be helpful to draw up at EU level a list of key enabling security technologies that are to be retained within the EU. Relevant initiative of this kind could be declared projects of common European interest (IPCEI).

The Federal Government will therefore

- ensure that Germany actively advocates completion of the single security market.

- work towards a situation whereby the entire gamut of key enabling security technologies is available from European suppliers. This would be interest of achieving greater strategic sovereignty for Europe and can be achieved by means of targeted industrial policy action at EU level.

10. Involving all of society in a debate on the security industry and its role in upholding domestic security, peace and stability

Much of the framework within which the civil security industry is operating in Germany is shaped by public debate about the industry and its relevance for our national, European, and transatlantic domestic and security policies. It is therefore important to have a debate with civil society about the constructive role that this industry is playing in keeping our society safe and free. People's reservations about new technologies must be taken seriously, but they must also be scrutinised. New and innovative security technology will only be widely used if there there is broad acceptance for it on the market and if the overall framework is conducive to innovation. Licencing requirements and liability rules that apply not least for the testing and use of innovative security solutions must be designed in a way that also takes adequate account of the needs of the market.

The Federal Government will therefore initiate

- a dialogue with representatives of civil society and from the security industry so as to discuss the role of the civil security industry and to create a framework that is conducive to innovation.