CSS Analysis in Security Policy

CSS ETH Zurich

No. 111 • April 2012

PPPS IN SECURITY POLICY: OPPORTUNITIES AND LIMITATIONS

Cooperation between public and private actors has become an important instrument of domestic security policy. Public-Private Partnerships (PPPs) take on essential tasks in protecting critical infrastructures, in cybersecurity, and in ensuring security of supply. However, difficulties in implementing such partnerships in the areas of coordination, expectation management, transparency, and ensuring coherence should not be underestimated.

Cooperation between public and private actors is becoming increasingly important in security policy.

Since the 1990s, the boundaries between the corporate sector and the state have become increasingly permeable. The policy of New Public Management set off a wave of privatisations in a broad variety of public services. The fundamental idea underlying this reform of the public sector is to harness the private sector's efficient production methods for the provision of public services. In this model, the authorities concentrate on political and strategic governance and leave the operative implementation to private actors. Against this background, so-called Public-Private Partnerships (PPPs) have been formed in a number of policy areas. The "PPP" label is applied to several forms of cooperation. It is generally used for long-term cooperation between private and public actors for fulfilling a public task.

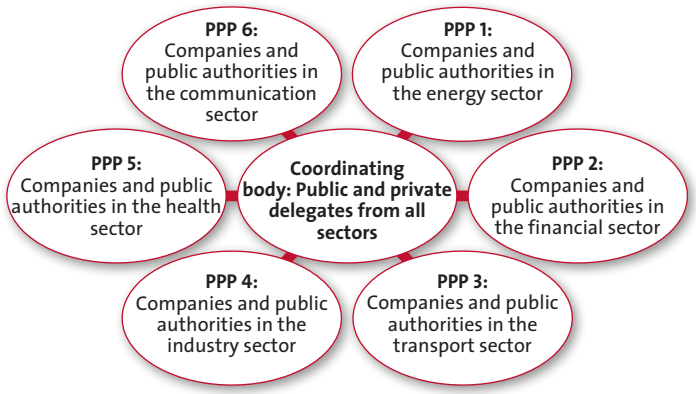
For a long time, there was little to be seen of this tendency to explore new forms of public-private cooperation when it came to security policy. Providing security is not just one of many services that the state must deliver. Because security is directly linked to the question of the monopoly on force, security policy is traditionally regarded as an exclusive domain of the state. Nevertheless, in this area, too, there is a tendency towards more cooperation between the corporate sector and the state. The most visible, but also the most controversial example of this is the outsourcing of military tasks to private security providers, as seen in the case of the US military.

Less attention is usually given to cooperation in the field of domestic security. However, such cooperation has become increasingly important. In many countries today, PPPs take on tasks in connection with civil protection. Examples include partnerships for Critical Infrastructure Protection, prevention of cyberattacks, or ensuring security of supply.

Increasing importance within security policy

Why do states increasingly seek cooperation with the private sector even in the sensitive area of domestic security? Two factors are decisive here. First of all, the increased cooperation is the result of economic liberalisation. Privatisation of state-owned businesses means that the government no longer has direct influence on certain companies whose services are essential for the functioning of the state. This can be seen clearly in the case of the telecommunication sector, which was long subject to direct state control. Governments were able to determine directly the security standards for the respective networks. In today's liberalised telecommunications market, the government can only exert indirect influence by intervening with regulation, offering incentives, or seeking cooperation with operators.

The "flower model": PPPs in the area of critical infrastructure protection



Source: Modelled on the organisational structures of the Centre for the Protection of National Infrastructure (UK)

The second factor contributing to the growing importance of PPPs in security policy is the complexity of the socio-economic environment. Modern societies are marked by a high degree of interdependence in a broad variety of sectors. For instance, if the power supply fails, this may easily result in the disruption of transportation systems, which in turn may mean that individuals are prevented from reaching their workplace, and thus certain important tasks are no longer carried out. The widespread use of information and communication technologies has even increased this interconnectedness and mutual dependence. Failures at neuralgic nodes can have cascading effects, the dynamics of which are very difficult to predict.

In the interest of optimising collaboration between various service businesses in case of a crisis, the authorities must know where the interfaces between the companies are. Civil protection requires integrated planning that can only be achieved with cooperative networks. One of the core tasks of civil protection, therefore, is to build partnerships in which the responsible representatives of businesses and of the authorities involved can prepare for potential crises.

Examples of cooperation

Cooperation between public and private actors is especially important in the protection of critical infrastructures. These are companies that ensure the availability of crucial goods or services (e.g., energy, transportation, or telecommunication). Many countries have developed comprehensive programmes in order to organise cooperation in this area. All these efforts revolve around the exchange of security-relevant information between the operators of critical infrastructures and the representatives of the public authorities involved.

Cooperation is usually organised by sector. This means that mainly companies and public authorities from the same economic sectors will exchange information about risks, trends, and possible protection measures. Coordination of the various sectoral partnerships is usually the task of a superordinate body that is, in turn, made up of public and corporate representatives form all sectors. This structured form of private-public collaboration may be described as the "flower model" (see graphic). The programmes for critical infrastructure protection in the UK, the Netherlands, in Australia, or in the US, for instance, follow this model or similar ones.

A similar logic determines the work of partnerships for cybersecurity. In these PPPs, too, the main intention is to exchange information. The business owners inform the authorities about which incidents they have registered, which possible security gaps they have identified, and which countermeasures they have taken. This allows the authorities to get a better picture as to threats and risks in the area of cybersecurity. In return, the companies are supported in incident prevention and in incident response. Because cyberspace knows no national boundaries, the authorities are in especially high demand when it comes to coordination with other countries. The strong mutual dependency between the state and the corporate sector in the area of cybersecurity has contributed to the enormous success of PPPs in this area. In almost all countries, PPPs are mentioned as important instruments for cybersecurity.

Programmes for critical infrastructure protection and for the promotion of cybersecurity are examples of newly established partnerships. The increased cooperation in the domestic sphere is also the result of an intensification of already existing forms of cooperation. In the area of supply policy, for example, such collaboration has a long tradition. One of the core tasks of the state is to ensure the supply of essential goods such as foodstuffs, raw material, energy, or medicine even during times of crisis. In the sphere of supply policy – which, in the case of Switzerland, is based on the experiences made in two world wars – the state sought cooperation with the providers of such goods at an early stage. The authorities have frequently intervened directly in the market, for instance by requiring the creation of mandatory depots for certain goods.

Today, rather than issuing regulations, the tendency is to ensure the security of supply by means of increased cooperation. In order to comprehend the complex national and international integration of the economy and construct an efficient supply policy based on that understanding, the authorities are dependent on cooperation with the private sector. Conversely, corporations also are interested in effective regulation. On the one hand, they wish to avoid unnecessary market intervention, while on the other hand, they themselves rely on the resources of other companies and are therefore interested in a high security of supply.

In a networked and dynamic environment, security cannot be ensured via regulations.

The example of Switzerland's National Economic Supply (NES) demonstrates how the policy of supply security – which was long dominated by the (supposed) antithesis of intervention and free-market principles – has evolved in recent years towards a collaborative partnership. The present structure of the NES is strongly shaped by the collaboration of militia staff from the corporate sector and the public administration. In total, more than 300 executives from corporations and the public sector are involved.

Their work is coordinated and structured by the Federal Office of National Economic Supply (FONES) as the responsible staff section. The representatives of companies and the civil service work jointly on developing precautions for contingencies. There is a realisation that neither the market nor the state can ensure the supply of essential goods to the population on their own without mutual support.

The prevalence of PPPs in the area of critical infrastructure protection, cybersecurity, and supply policy shows how important public-private cooperation has become in security policy. It is essential to understand that Public-Private Partnerships in the policy field of domestic security do not serve to privatise security policy-related tasks, but constitute a complement and alternative to regulative state intervention. In a strongly networked and dynamic environment, security can no longer be ensured effectively via regulations. A focus on the shared interest in a secure and calculable environment can be useful for bridging the gap between security and economic considerations that does occasionally come to the fore.

Challenges and limitations

The difficulties in implementing a partnership approach in security policy should not be underestimated. Two major challenges can be identified in practice. First of all, the cooperation can only be a fruitful one if it is well coordinated. This involves a number of tasks. First of all, all relevant actors must be convinced of the value of cooperation. Then, joint goals and approaches must be agreed upon, and participants must determine who will be responsible for implementing which measures. All of these steps harbour a strong potential for conflict and must be discussed in sometimes protracted processes. Therefore, actors are required who will coordinate, structure, and advance this cooperation in substantial terms. These actors may be drawn from either the public or the private sector. What matters is that they must have at their disposal the necessary resources for managing the partnership and be acknowledged as organisers of cooperation by the other partners.

Cooperation can only be fruitful if it is well coordinated.

The second challenge is external communication. The great potential ascribed to the concept of public-private collaboration creates expectations that are occasionally very high. Both representatives of public bodies and the delegates of private companies are accountable to their superiors. It is sometimes difficult to gain a sympathetic hearing for the fact that concrete results may be long in coming. Because many companies operate internationally, there may be an additional challenge in convincing management of the importance of national or even local collaboration.

In addition to these practical challenges, another decisive factor is that cooperation must also respect democratic principles. Even if it is legitimate for authorities to cooperate primarily with immediately security-relevant companies, this may not lead to distortion of competition. Additionally, a minimum of transparency must be ensured even in partnerships where sensitive information is exchanged. Representatives of public bodies must ensure that the PPPs do not operate outside of democratic control mechanisms, and that they are able to report to their respective democratic oversight body on their activities.

In the implementation of a partnership approach, it is crucial that cohesion in security policy not be lost. Setting priorities in security policy and implementing defined policy measures remains the task of the government. PPPs can be a promising instrument in this context, because cooperation is often more effective than regulation. However, collaboration requires that the government preserve its independence vis-à-vis private interests and steer and coordinate PPPs in a way that serves overarching goals of security policy. This is the only way to ensure that a partnership approach in security policy is successful and remains acceptable throughout society.

PPPs in practice: Exemplary activities in the sphere of cybersecurity

- **Incident support:** The network of PPPs is used to analyse an incident (virus, hacker attack, etc.) and to define technical countermeasures. If required, public actors offer support in initiating legal measures or in coordination with foreign authorities.
- **Early warning:** Via internal communications channels, members are swiftly informed about attacks on other members. this allows them rapidly to initiate countermeasures, if required.
- **Workshops:** In regular meetings, members are informed by experts about new dangers and protective measures against cyberattacks. These workshops not only promote the exchange of professional information, but also help to strengthen mutual trust.
- **Public relations:** Members are jointly engaged in educating users of internet services about potential dangers. This joint approach enhances the credibility of warnings.

PPPs in Switzerland

There are a number of examples of successful cooperation between the state and the corporate sector in Switzerland in the field of security policy. In addition to the FONES, the critical infrastructure protection programme of the Federal Office of Civil Protection (FOCP) is also based on public-private collaboration. Another notable example is the Reporting and Analysis Centre for Information Assurance, which focuses on the protection of critical information infrastructures.

These functioning partnerships between public and private actors reveal the potential of collaboration in Swiss security policy. In an international comparison, conditions in Switzerland are particularly favourable for this approach. Whereas in many other countries, the relationship between the state and the corporate sector is marked by strong mutual distrust, which often obstructs cooperation, this problem is noticeably smaller in Switzerland due to the militia system and the country's small geographic expanse. In fact, there are a number of cross-sectoral networks that can be used for cooperation.

The main challenge in implementing the PPP approach in Switzerland is the strongly developed federalist system. The sharing of tasks between the federal administration, the cantons, and communities may cause the allocation of responsibilities among public authorities to be unclear. However, collaboration with the private sector can only be successful if there is clarity regarding which actor from the public sector is the correct contact person for businesses. Therefore, implementation of PPPs requires careful

coordination between the various administrative entities. In this respect, it may be useful if one actor is awarded a clear mandate for coordinating partnerships in a concrete field of security policy.

It would be a welcome development if the cooperative approach were taken into account as far as possible in the formulation of future domestic policy. This requires clear requirements for the individual public authorities to promote and implement collaboration with the private sector. It is precisely because the instrument of PPPs has so much potential that it must be applied carefully and responsibly.

- Author: Manuel Suter
  suter@sipo.gess.ethz.ch
- Responsible editor: Daniel Trachsler
  sta@sipo.gess.ethz.ch
- Translated from German:
  Christopher Findlay
- Other CSS Analyses / Mailinglist:
  www.sta.ethz.ch
- German and French versions:
  www.ssn.ethz.ch

Previous issues