SETTING THE SCENE "Auditing security and defence – Risks, approaches and tools"

Ladies and gentlemen, it is now up to me to set the scene on which we will soon be raising the curtain, with the first introductory briefing. I will do my best to keep from giving you any spoilers of the briefings to come from the many presenters who will take the floor in turn, but I would still like to sketch out for you what, to my mind, are the challenges of public external auditing in the security and defence field.

To give you a sense of who you have before you, allow me to introduce myself briefly. Having trained as an engineer, a lawyer and an auditor, I have had the opportunity over a career spanning more than forty years to familiarize myself with nearly all the viewpoints of the speakers who will take the floor over the course of this seminar – as an officer in the French Navy for roughly a decade, an adviser to the French Minister of Defence, a leader of a public industrial institution and a national civil-military aerospace research agency, a public auditor, and finally first a member, and later the president, of the International Board of Auditors for NATO for nearly eight years. So what I am going to share with you now is none other than the product of my extensive observations and experience of the world of defence, on the one hand, and of national and international auditing, on the other.

To set the scene, as the title of this briefing compels me to do, we must start out by talking about the space and the actors.

The SPACE is vast and complex.

The national and international defence and security sector covers a field stretching from policy, parliamentary and government initiatives to purely operational activities, industry programmes and support activities. Each of these secondary fields contributes overall to a collective security and defence strategy. Yet each of these fields also has its own logic, values, organizational and behavioural culture and, as it interacts with each of the others, generates the particular complexity of the world of security and defence.

To present this space as the interface between the policy field, the resources field and the action field might suggest that there is nothing all that special about it compared, for example, to the entrepreneurial space of a major industrial or commercial multinational corporation. It seems to me, though, that one of its particular characteristics has vital effects: the continuous interaction of each of these fields with the others and, between them, the interaction of the (often highly powerful) forces passing through each of these fields.

In the policy field, where a security strategy and objectives become established, no actor in a democracy is entirely free, and governance remains especially complicated: the legislative branch, the executive branch and opposition forces of all kinds (unions, intermediaries in general, public opinion) play a game together in which the pure rationality of security and defence can be supplanted by decisive, psycho-sociological or interests-based rationalities.

The same goes with resources; firstly, those that are subordinate to policy decisions but also have varying, even divergent tensions running through them: what government hasn't had to take decisions on equipping its security forces by making the social, diplomatic and industrial impact of its choices its prime consideration? What industrial would not try to sell its most profitable technology rather than the one that will meet the basic needs of its customers? Do the amount and quality of resources solely reflect a logic of operational effectiveness, or rather do they occasionally serve symbolic intentions of power or authority, and what is possible rather than necessary? This can be said to be true in all fields of public policy, but I remain convinced that the field of security and defence – potentiated by the primary consideration of life and death, citizens, nations, but also the sometimes considerable powers of the players in the game – more than any other field is subject to such tensions.

So this is my first remark, in the form of a consideration for auditors: to paraphrase Dante, abandon all hope ... of being able to apply a simple, unequivocal rationality to your work, your analyses or your recommendations.

THE ACTORS are obviously many and especially varied – politicians, diplomats, military personnel, lawyers, industrialists, etc., categories that can be broken down further into a great many sub-categories. But I think this short, simple list is sufficient to touch upon the importance of the paradigm of the organization, or to put it more simply, its ORGANIZATIONAL CULTURE. Each of these actors understands, contributes to, and responds to the requirements of a security strategy and collective security objectives, as well as the requirements specific to auditing, in a different way.

The primary characteristic of the socio-organizational culture of the defence sector is the extreme strength of this culture, which hardly cedes an inch in the face of entreaties or interference from other systems of representation and thought. The reason for this clearly has to do with the aims; in short, when preserving lives or winning a war is at stake, it is harder to conceive of straying from the path of an effectiveness that has been deeply, patiently encapsulated in mental and behavioural paradigms that have proven their worth. And yet, basically, this works. So while concessions may be made here and there, a sort of self-discipline emerges to counter the effects of any autonomous cultures that might be too counter-productive. As a corollary to my initial remark for auditors: the first effort to be made is therefore to analyse and understand under what conditions a socio-organizational meta-culture will gather actors that might appear culturally very different into effectiveness. In other words, why and how a politician and a soldier, a soldier and a lawyer, a politician and an industrialist, and others will talk to each other and can understand each other, for the auditor to ultimately be able to hear them (this being the etymological role of the auditor), to understand them all and to say something to them whose intention will be understood by everyone in the same way.

It is no secret that this becomes more complicated when moving from the national level to a multinational space. Regardless of how collective decisions are taken, regardless of the *affectio societatis* of the members of the multinational organization, the concept of the nations' sovereign interest and the political and operational system produced by it in effect create additional spaces of rationality, other layers of meta-culture, and meta-discourses, which further complicate the auditor's work. This can range from major decisions on collective strategic programmes (for example, the sometimes inefficient consequences of the distribution of industrial shares as part of multinational cooperation equipment programmes), to purely anecdotal operational aspects in the field.

The space and the critical factors of multinational action on defence are fundamentally political: no matter what collective oaths are taken or alliances forged, what nation, when its back is to the wall, can readily agree to put its security, its defence and its vital interests fully into the hands of others? That doesn't mean that the security and defence field is doomed to relative powerlessness by the nations' selfish interests, coupled with a fatal inefficiency, the latter issue moreover being fundamental to auditors. But to make a meaningful, useful contribution through their observations and recommendations, the auditors' path narrows further given that an undisputed, shared, collective culture of security and defence has not managed to become an imperative. Faced with security principles, public policy standards and performance criteria that differ from north to south and from east to west, auditors are obliged to rely on the least common multiple, and accept the professional frustration that the auditors in all international organizations have to get used to in order to survive.

Finally, before we move on from this general introduction, one of the major, critical, practical characteristics of security and defence is that control over information, with its operational ramifications of confidentiality and security, is a strategic factor. This fact – and this is something of an understatement – is not without consequences for auditing.

So there you have the scene and the actors. Now I will take a few more minutes to talk about the interplay.

The interplay in which the public auditor is involved, to keep it as simple as possible at this stage of our seminar, can be broken down into three acts: audit planning, performing and reporting. In each of these acts, when the scene takes place in the field of security and defence, the auditor and the audit itself face risks of varying natures: political, cultural, methodological, technical, and more. When I talk about risks, naturally I mean situations that can sap the auditing activity of all or part of its effectiveness and usefulness.

Here, I would already like to draw a distinction between financial auditing and all other forms of auditing. General-purpose auditing of financial statements, which has a generally legal formal basis essential for all the actors in the complex space I have just described and moreover is largely technically objectifiable, in most cases is not, at least insofar as audit planning and performance are concerned, much more problematic than in most national or international public organizations, except of course with regard to the effects of a low appetite for auditing in the operational world of security and defence overall. We could also consider the very specific yet very different cases in which the international or multinational body has not unambiguously defined its financial reporting framework, which poses obvious problems of normative references for the auditor, or the case of a very high level classification affecting the body's operations being necessary for any outsider's access, up to the point where it may sometimes hinder the auditor's ability to observe and draw conclusions. But for the context that interests us today, the first case is exceptionally rare and the second gives rise to the same kinds of comments as those I will now make, with regard to managing confidentiality, about the other major field of auditing: performance auditing (of all kinds).

A common denominator in all the risks and challenges that auditors face, confidentiality, and by extension, transparency, is central and crucial, insofar as it causes a range of significant difficulties (legal, methodological, technical or logistical). Not all information in the field of security or defence is classified, far from it, but a lot of it is, and the chances increase when you move away from administrative or operational routine. And even when the information is not defence confidential, there are many cases where other forms of confidentiality related to security programmes apply: industrial and commercial confidentiality, staff management confidentiality, and even informal confidentiality, which is the hardest to assess and manage, as it is about safeguarding the political interests of states or their partners. In principle and thanks to the international auditing standards generally accepted by all democratic countries, public sector external auditors have unrestricted access to the information and people required for them to conduct their audit and form an opinion, meaning that they have a "universal right to know" as part of their mandate. But we make no secret of the fact that this principle has its limits in the security and defence sector. The requirement for auditors to have clearance to access classified information, at a more or less high level (confidential or secret) means that it is very difficult to manage the auditing staff; because of increasingly cumbersome and strict procedures for accessing and retaining information, the higher the level of classification, the more careful and effective the auditors must be in the way they plan the availability of their resources, both in terms of quality and quantity, to be able to effectively manage the scheduling and the scope of their audits; logistically, there are access restrictions to certain sites or people, imposed bans sometimes on using your own equipment (computers, telephones, software, etc.), the requirement to use the auditees' own tools with no guarantee that files will remain confidential (though this is normally guaranteed as part of the absolute inviolability of the work of independent auditors). All these factors and many more impose material constraints on auditors in the security and defence sector, which they might well be able to overcome (in which case the scheduling and planning of missions is complex) or might not (in which case there is a risk that the auditing process and the possible recommendations become relatively ineffective). In some cases, this leads to audits being aborted. The greatest risk with this is that auditors censor their own auditing strategy because of the complexity involved. Case in point: to conduct audit fieldwork in high-risk zones, such as Afghanistan and Iraq currently, and irrespective of the moral requirement to only have volunteer auditors do the work, under NATO's regulations, civilian personnel are required to have clearance for deployment there; such clearance is only granted at the end of a week-long training course, for which you have to register months in advance. In these conditions, the cyclical lack of cleared auditors may lead to some audits not happening, even though they are deemed strategically important. The logistical and technical preparation and planning of security or defence audits are absolutely crucial to their efficiency and success.

However, during the planning phase, the risk of self-censoring is not always caused by the anticipated material, logistical or technical difficulties. The complex interplay of the actors, which I mentioned earlier, may also contribute. In general, qualifications, criteria and performance indicators are essential. When actors have different and even irreconcilable ideas about the performance of a policy, a programme or a project to which they contribute, the auditor may have to resort to the least common multiple of understanding that I was talking about earlier. The risk is giving up when the least common multiple cannot be reasonably defined because of conflicting performance criteria, or when its scope is too restricted to reach useful conclusions or to warrant the use of rare and costly auditing resources (time, money, people).

There is also the issue of auditing particularly sensitive security or defence issues that could potentially jeopardize the reputation of states, security forces or industrial partners. Auditing sensitive sectors or topics is always a problem. But when it comes to security, credibility is a cornerstone of efficiency, and the defence of vital interests, whether national or international, military or industrial, or of another nature, may lead some actors to prioritize performance over other principles (rigour, lawfulness or even public morals). Then there are the not-just-theoretical hostile situations in which auditors are pressured or even directly or implicitly threatened. This happens when an auditor is sure he or she can help better serve the public interest, even if this entails major difficulties in managing confidential information. In such situations, auditors are faced with a dilemma, which the auditees are actually glad to leave to them: either tackle these sensitive issues for the benefit of democracy and transparency (often promoted by political decision-makers) with the risk of undermining wider-reaching supreme interests, or simply give up.

Once these obstacles are overcome, you still have to perform the audit and draw up observations and findings.

There are many factors that make it hard to conduct smooth and efficient security/defence audits. I will mention them briefly, not because they are set in stone but because they can support our discussions. Some of those factors are well known for being restrictive, and some are cultural factors that should be taken into account to improve the efficiency of audits.

- Because auditees have various, not necessarily converging, interests, their attitude and contribution to audits are also very different. Because of such behavioural differences, audits are hard to plan, risks are hard to assess and quality control processes are hard to define.
  There is one major difficulty that directly reflects this diversity: condensing in one single document findings and recommendations that will obviously not get the same reception from everybody. Not everyone will show the same interest and desire to respond to the recommendations to improve the OVERALL performance of the system; again, you need to find the right angle, content and tone to bring together all the energies. The force of all the national organizational cultures involved (civilian, political, military, operational, at different levels) makes this extremely hard to achieve. In my experience, I think it is fair to say that the drafting and delivery of a message and the setting out of useful, applicable recommendations is the most important and the most sensitive phase of auditing in the field of security and defence.
  In this respect, note that benchmarking studies, which could ensure that everyone agrees on the best – or at the very least good – practices, are in actual fact often ineffective,

since it is hard to find practices that are sufficiently relevant, either operationally or culturally.

- More specifically, in auditing, the culture and management specific to the military constitute major risk factors.

  A strong hierarchical culture has a significant, direct impact on how the auditees behave: when strict chains of command are in place it is often harder to access information, especially when the superiors wish to keep control of the information given to the auditors despite the principle of unrestricted access to information. People, especially on the lower rungs of the hierarchy, may not handle the observations or criticism very well if they are afraid of being reprimanded, even though auditors are neutral, unbiased and always impartial in this respect. External auditors can sometimes be mistaken for inspectors, which further complicates the contradictory processes, which become biased and a lot more defensive than in other sectors.

  One last, practical point: there is generally a rapid rate of turnover in military human resource management, sometimes leading to insufficient background knowledge and thus both shortfalls in the auditing process and insufficient follow-up to the audit recommendations.

I must wrap up now. I apologize if I have spoken for too long. I hope I have managed to shed some light onto some problematic areas and that the European Court of Auditors will be able to share a wide range of experiences with all the practitioners who will be talking today and tomorrow. I will end by simply saying that in the field of security and defence, more than in any other area subjected to external auditing in the public institutions sector, there needs to be a form of creativity and open-mindedness (in terms of methodology, tools and probably even auditing philosophy) without which the complexities and powerful underlying cultural and organizational paradigms could make the auditors ineffective, useless and ultimately discouraged.

Thank you very much for your attention.