Summary Report | 29th SSF Security Talk

‘Posture – la volonté ne suffit plus’

Welcome Address

Major General (retired) Claude Meier, President of the ‘Association de la Revue Militaire Suisse (ARMS)’ & President of the ‘Centre d’Histoire et de Prospective Militaire (CHPM)’

Major General (retired) Claude Meier welcomed the participants to the 29th SSF Security Talk – the first event organised by the SWISS SECURITY FORUM in French-speaking Switzerland. He began by highlighting three key aspects of the topic of security policy ‘posture’.

Firstly, the geostrategic and security situation has changed fundamentally, although this realisation has not yet taken hold across society as a whole. War on the European continent, hybrid threats, disinformation, cyber-attacks and increasing geopolitical tensions also present Switzerland with new challenges.

Secondly, it is illusory to believe that security and stability are guaranteed in the long term. Security must be actively worked towards. Comprehensive protection is no longer possible in an interconnected and therefore vulnerable world.

Thirdly, therefore, what is crucial is the ability of the state, the economy and society to manage crises, remain capable of acting and persevere in the long term. This requires not only robust and resilient structures and infrastructure, but also a shift in societal mindset: “Il faut passer d’une culture où tout est considéré comme acquis à une culture de responsabilité individuelle et de capacité de défense.”

Keynote Presentation

Dr Alexandre Vautravers, Scientific Director of the ‘Centre d’Histoire et de Prospective Militaires (CHPM)’

Dr Alexandre Vautravers opened his keynote address with an analogy between health and security. As long as one is well, such issues are regarded as secondary and decisions are put off until later. However, should an incident occur, priorities change abruptly and what were once considered minor details suddenly become crucial. Security, just like health, is by no means a given: “La sécurité n’est jamais acquise.” The notion of permanently guaranteed peace is an illusion.

According to the International Committee of the Red Cross (ICRC), there are over 120 armed conflicts worldwide. Their direct and indirect effects ultimately affect the entire world population. Vautravers pointed to a fundamental difference in the perception of war and peace: whilst a generation in Switzerland had grown up for whom war was largely an abstract concept, there were generations elsewhere who, , had experienced nothing but war and could themselves scarcely imagine what peace meant.

Ultimately, the credibility of the rules-based international order is at stake in the war in Ukraine. Following the collapse of the Soviet Union, Ukraine had renounced its nuclear weapons in exchange for security guarantees. A loss of confidence in such guarantees could have serious strategic consequences. Vautravers expects that, over the next five to twenty years, numerous other states could develop nuclear weapons to protect themselves against military attacks.

The peace dividend of the 1990s and 2000s led to the emergence of so-called "armées bonsai" in Europe. Vautravers illustrated this using the image of a bonsai: "À la fin, vous avez la même forme que l'arbre. Mais vous n'avez pas l'ombre et vous n'avez certainement pas les fruits." On paper, the armed forces possessed a wide range of military capabilities; in a crisis, however, they lacked the scale, capacity and staying power. Using Sweden as an example, Vautravers highlighted the discrepancy between the speed at which military capabilities are being dismantled and the speed at which they are being rebuilt. Whilst Sweden had reduced its army from 82 to seven mobilisable battalions within three years, it now takes around ten years to build up a single additional brigade. Among other things, there is a shortage of instructors, training facilities and simulators.

Vautravers also viewed with concern the widening gap in defence spending between Switzerland and its European partners. Whilst NATO member states aim to spend five per cent of their gross domestic product (GDP) on defence and security-related expenditure by 2035, Switzerland is targeting just one per cent by 2032. This discrepancy also raises questions regarding future capacity for cooperation. Vautravers drew parallels with Switzerland's situation in the 1930s: despite the mobilisation of considerable financial resources, urgently needed tanks and aircraft could not be procured and made operational in time due to geopolitical developments.

Against this backdrop, what does a credible security 'posture' entail? The clear distinction between war and peace no longer exists: "Il n'y a plus de situation de guerre. Il n'y a plus de situation de paix. Il n'y a plus de frontière entre l'un et l'autre." Rather, we are operating within a continuum in which competition can turn into rivalry, rivalry into confrontation, and confrontation ultimately into war – without a formal declaration of war. In this context, Vautravers referred to Clausewitz, who argued that war is the continuation of politics, rivalry and the struggle for power by other means.

It is against this backdrop that hybrid warfare must also be understood. Vautravers explained its different conceptual origins in the USA and Russia. The Russian concept, in particular, is based on the idea of countering the West's military superiority through the targeted use of non-military means. Hybrid warfare accordingly aims to achieve political and military objectives using a broad spectrum of instruments.

The fact that hybrid warfare has long been a reality can now also be statistically demonstrated on the basis of the systematic recording of relevant incidents in Europe. Whilst shopping centres are targeted in some countries, in others the targets are transport or energy infrastructure, as well as arms and munitions factories. The variety of targets suggests that the specific strengths and weaknesses of individual countries are being systematically analysed and exploited in order to achieve a particular effect.

In conclusion, Vautravers outlined three possible scenarios for the development of the war in Ukraine: firstly, a freeze in the conflict, which could continue to preoccupy Europe for decades; secondly, an intensification of the military conflict, which he assessed as the least likely scenario given the limited prospect of a decisive impact from the deployment of additional missiles and drones; and thirdly, a geographical expansion of the conflict beyond Ukraine. In doing so, he made a clear distinction between intensification and expansion: "Je n'ai pas dit l'intensification du conflit, mais l'extension du conflit." He left it to the audience's imagination to work out what this would mean.

Brief statement
Major General Raynald Droz, Commander of Territorial Division 1 (Ter Div 1) of the Swiss Armed Forces

At the outset, Major-General Raynald Droz painted a picture of a soldier upon taking up duty. That soldier's conduct, he said, already provides the answer to a fundamental question: "Peut-on compter sur lui?" This question arises just as much in the case of a formation, a military staff or the entire army, and lies at the heart of military 'posture': "C'est la cohérence entre ce que nous affirmons, ce que nous préparons et ce que nous sommes réellement capables d'accomplir." The will to defend one's own country, protect the population and preserve freedom remains indispensable, but is not sufficient on its own. Only the translation of this will into an actual and permanently available capacity for action lends 'posture' its credibility.

We are still fortunate enough to be able to train. However, this comes with a considerable responsibility: the time available must be used to test capabilities and address existing shortcomings. Preparation only becomes credible when one is prepared to measure one's own capabilities against the difficulty of the mission. This requires courage on the part of leaders – the courage to set standards, to admit shortcomings and to demand that they be rectified.

Reliability begins with simple actions and daily discipline. However, this must go hand in hand with personal initiative: "Une armée fiable est donc une armée dans laquelle chacun sait ce qu'il doit accomplir, pourquoi il doit l'accomplir et quelle responsabilité lui revient." This reliability produces two crucial effects: trust and deterrence. Whilst the population must be able to rely on its army, a potential adversary must factor its actual capabilities and resolve into its calculations.

At the same time, the credibility of the military 'posture' depends to a large extent on civilian partners. The interfaces between the army, the authorities and the business sector are therefore crucial. Responsibilities, tasks and priorities must be jointly clarified and practised well before a crisis arises. National resilience arises where everyone knows their responsibilities and is prepared to fulfil them even under difficult conditions.

A credible military and security 'posture' ultimately rests on three commitments: being prepared, being reliable and being able to persevere. Droz concluded with an appeal to each individual's

sense of responsibility: “Je connais mes responsabilités, je m’y prépare et on peut compter sur moi.”

Brief statement
Christoph Gerber, General Manager, ELCASecurity & President of the ‘Groupe romand pour le matériel de Défense et de Sécurité (GRPM)’

Christoph Gerber opened his remarks with the image of two Swiss customs officers from an earlier advert, who were wondering why nothing ever happened on their watch, whilst goods were being smuggled across the border behind their backs. He said the current situation reminded him of this: awareness of the current threats is still not sufficiently widespread amongst the general public.

From a cyber security perspective, hybrid warfare has long been a reality: “Ce n’est plus une menace probable. C’est ce qu’on vit au quotidien.” It is now almost impossible to draw a clear distinction between cybercriminals, activists and state actors. Consequently, Swiss critical infrastructure is also being targeted by cybercriminal groups operating with state tacit approval.

Of particular concern is the increasing interconnection between the digital and physical worlds. Cyber-attacks no longer aim merely at data theft or paralysing systems, but at deliberately altering their behaviour. Gerber cited the manipulation of the cooling system for blood reserves in a French laboratory. In the case of interconnected energy supply systems, even private end devices could indirectly become a gateway for attacks on critical infrastructure.

The answer to this lies in the military principle of defence in depth. This begins with raising awareness and training the population. The ability to detect enemy activities, pick up even faint signals and anticipate threats is also crucial. It is precisely in this area, however, that there is a lack of information exchange between the private sector and the state.

In view of the current, state-sponsored technological arms race, Gerber also drew parallels with the year 1936. A credible deterrent requires actual capabilities. In the spirit of the former total defence concept, a capable domestic industry is therefore needed. For in times of crisis, borders close and trade becomes more difficult: “Ça ne suffit plus de faire marcher la planche à billets. Il faut avoir des éléments de troc.”

Gerber feels that the 2026 Security Policy Strategy fails to give sufficient weight to domestic industry. Without its own industrial capabilities, Switzerland risks facing a fatal dependence in the event of an emergency: “Le jour où notre armée aura besoin de son industrie, à ce moment-là, il faudra juste prier pour que les États amis ou voisins ou alliés nous aident.”

Brief statement

Aude Pugin, CEO, APCO Technologies & Vice-President of the Federal Commission for Space Affairs (CFAS)

In her statement, Aude Pugin highlighted the strategic importance of space and its dual nature – both civil and military applications. She noted that the Swiss space industry possesses key competencies across the entire value chain, which contribute significantly to the country's strategic autonomy.

Space has long since become a critical infrastructure: "Le spatial, c'est le chemin de fer du 21e siècle." Just as the railway once transported goods, space today transports information on which the economy and society are heavily dependent. Any disruption to space-based services would have far-reaching consequences for navigation, synchronisation and communication systems. Space infrastructure is also indispensable for modern armies – from satellite-based reconnaissance and strategic early warning, through secure communications, to command and control and target acquisition.

In view of growing geopolitical tensions, Europe's strategic autonomy is becoming increasingly important: "Les alliances d'hier ne sont plus celles de demain." Even the access to space currently guaranteed by private American providers such as SpaceX can no longer be taken for granted. This makes European cooperation in building up its own space capabilities all the more important – both in terms of autonomous access to space and in terms of sovereign space infrastructure. Pugin referred to projects such as the European Ariane 6 launch vehicle, the reusable spaceplane VORTEX and the ALPSTAR consortium, initiated and led by Switzerland. Such collaborative projects strengthen the strategic autonomy of the participating states whilst also offering Swiss industry the opportunity to play a key role.

Building an independent space infrastructure is costly, ambitious and technologically demanding. It can therefore only succeed through cooperation with European partner states and with significant involvement from industry. International cooperation serves precisely to further one's own strategic autonomy. At the same time, Pugin emphasised the economic added value of such investments: "Beaucoup de programmes de défense ont aussi permis de créer des capacités industrielles et économiques qui servent non seulement pour la défense du pays, mais aussi pour la prospérité de notre pays."

Panel discussion

In the concluding panel discussion, moderated by Major General (lib) Claude Meier and Fredy Müller, Managing Director of the SWISS SECURITY FORUM, Major General Raynald Droz, Christoph Gerber and Aude Pugin, together with National Councillor Isabelle Chappuis (Die Mitte, VD), a member of the National Council's Security Policy Committee (SPC-N) and President of the Swiss Civil Protection Association (SZSV), discussed the prerequisites for a resilient and effective Switzerland and the development of a credible security 'posture'.

In her political analysis of the preceding presentations, Isabelle Chappuis began by highlighting a key insight: peace is not the natural state of history, but is fragile and worth protecting. Security must not simply be delegated to the army, but is everyone's responsibility. However, awareness of the existing threats is still not sufficiently developed, even in political debates in Bern. During the coronavirus pandemic, there was much talk of 'business continuity'. Today, we must instead be thinking about the continuity of the state. 'Just-in-time' must be replaced by preparation in the spirit of 'just-in-case'.

In the face of new forms of attack, new defence strategies are also required. 'Situational awareness' is crucial in this regard, and space technology plays a key role in this. In this context, Chappuis criticised the Federal Council's decision to opt out of the European Earth observation programme Copernicus for the time being, for reasons of cost-saving. Whilst this would save 36 million Swiss francs, the Swiss economy would, according to the Federal Council, lose out on 51 million Swiss francs.

Strengthening defence capabilities

Fredy Müller began by referring to Major General Droz's remarks on shared responsibility and well-established interfaces between security actors. Is Switzerland on the right track in this regard?

Droz emphasised that the army was very well aware of its capabilities, but also of its limitations. Today, he said, it was not just a matter of strengthening the army, but of strengthening security as a whole – and thus of pooling the capabilities of all security actors. As a positive example, he cited the preparations for the 'Colibri' army operation in the context of the G7 summit, during which the army, together with the cantonal police forces of Geneva, Vaud and Valais, had run through possible threat scenarios in a 'wargame'. Crucial to this had been the building of mutual trust, but also the willingness to disclose one's own capability gaps and to ask other partners for support. Limited resources are effectively forcing security actors to pool their capabilities and efforts.

In light of the dramatic events in Ukraine, Fredy Müller asked Isabelle Chappuis, President of the Swiss Civil Protection Association, how well prepared the civil defence and emergency services in Switzerland are. Isabelle Chappuis noted that the Swiss civil defence had repeatedly demonstrated its capabilities in managing disasters, for example in Blatten or Crans-Montana. However, she added, it is not prepared for a war situation. Unlike in the case of a disaster of limited duration, the focus here is on long-term sustainability. Whilst the target in the 1990s was to have a strength of over 500,000 civil defence personnel, the current figure is barely 50,000.

In response to Claude Meier's question about specific measures to restore the necessary numbers, Chappuis referred to amendments already made to the Civil Defence and Civil Service Act, as well as work on a new compulsory service system. The democratic process, however, takes time, whilst crises are simultaneously accelerating.

Protection of critical infrastructure and economic resilience

Meier then steered the discussion towards the vulnerability of critical infrastructure, particularly the energy supply.

Aude Pugin recalled the impact of the COVID-19 pandemic and the war in Ukraine on international supply chains and commodity prices. She noted that the pandemic had heralded the end of 'on-demand, low-cost' supply chains. Resilience and strategic autonomy have become key concepts for industry. The crucial question is which goods and resources are strategically relevant and which must be accessible at all times. The energy supply is of particular importance in this regard. Whilst the renaissance of nuclear energy was initially driven primarily by climate policy, the question of sufficient energy capacity is now increasingly coming to the fore.

Gerber added that many sectors still operate according to the principles of peacetime logistics. However, these quickly reach their limits in crisis situations. The interdependence of digitalisation and energy supply, in particular, creates significant vulnerabilities. Just as in sport, crisis management must also be practised regularly. A simulated power cut quickly reveals how capable an organisation actually is of taking action, how long its fuel supplies will last and whether its emergency generators are working. We currently have a system that works excellently in good weather, but we are still not sufficiently prepared to anticipate difficult situations and practise dealing with them.

When asked about the corresponding challenges facing the army, Droz first pointed to a lack of reserves, for example in ammunition and weapons. These now need to be replenished at a time when international demand is particularly high and Switzerland, as a non-member of NATO, is at a disadvantage when it comes to procurement.

There is also a significant discrepancy between the number of critical infrastructure sites requiring protection and the available personnel. Comprehensive protection is simply not possible. This raises a key question in any planning process that nobody wants to answer: that of prioritisation. Whilst the focus had long been predominantly on disaster scenarios, it is now possible to discuss defence scenarios with the various partners as well.

Meier then addressed the responsibility of critical infrastructure operators. Droz described the difficulties of cooperating with foreign operators, some of whom refused the army access to their security plans. At the same time, even identified vulnerabilities sometimes persisted for years. Responsibility for protection lay primarily with the operators; ultimately, however, it was also a shared task. However, the resources available to the police and the armed forces were not sufficient to provide comprehensive protection for all critical infrastructure.

Referring to Chappuis' book *Notre liberté de penser*, Müller then addressed the digital threats to the economy, society and democracy. Chappuis highlighted a fundamental gap in the country's economic security: whilst energy requirements are defined in kilowatt-hours and food

requirements in kilocalories, there are no comparable criteria for digital supply. Digital dependence on other countries is a cause for concern, particularly as digital systems influence not only the functioning of society but also human perception and thought. She therefore also took a critical view of the fact that the tender for the Swiss Government Cloud was aimed at international technology conglomerates, even though the relevant expertise is also available in Switzerland.

Müller asked Gerber whether Switzerland was now sufficiently well-equipped following the creation of the Federal Office for Cyber Security (BACS) and the Cyber Command. Gerber acknowledged the significant progress made in recent years. However, the 'last mile' was still missing, particularly the financial and human resources required for operational implementation. Just as with compulsory stockpiling of essential goods, consideration must also be given to digital reserves, such as maintaining capacity in data centres or reserves of graphics processing units (GPUs).

Pugin added that, in addition to government investment, substantial investment from the private sector was also necessary. Using APCO Technologies as an example, she illustrated how a culture of security could be established within a company through information security standards, regular penetration tests, anti-phishing campaigns and training. She emphasised that the constant reinforcement of even seemingly self-evident rules of conduct was crucial in this regard.

In response to Müller's enquiry regarding staff acceptance of such measures, Pugin noted that cybersecurity was met with understanding, partly due to the private use of digital technologies. At the same time, she warned against over-regulation. Tackling new challenges was already placing a considerable strain on companies' human and financial resources. Regulations should therefore be based on the expertise of relevant specialists.

Strengthening societal resilience

In the third section, Meier raised the issue of risk awareness amongst the general public and their preparedness for potential crises.

Chappuis began by once again highlighting the numerous micro-enterprises that had no emergency plans whatsoever for power cuts or cyber-attacks. Whilst this was understandable given their day-to-day challenges, it was nonetheless problematic: "Notre économie est une infrastructure critique." Understanding of security policy issues also varied greatly amongst the general public. People were still in a phase of raising awareness.

Droz then mentioned the societal 'comfort zone' in which Switzerland finds itself. The population has become accustomed to an exceptionally high standard of quality and supply. Even a brief power cut or a temporary restriction on their usual comforts is quickly perceived as a scandal. In a crisis, however, the initial priority is to ensure a minimum level of provision: "Le minimum et pas le maximum." Resilience then means returning to the original level as quickly as possible. On the

other hand, the willingness of young members of the armed forces to take on responsibility and, in an emergency, to put themselves at personal risk is encouraging.

Müller concluded by addressing the issue of individual crisis preparedness. People who prepare for potential crises by stockpiling emergency supplies or taking other precautions are sometimes ridiculed as 'preppers'.

Chappuis referred to a newspaper article in which she had been described as the nation's 'prepper'. However, she emphasised that she was by no means concerned with individual survival strategies for lone fighters, but rather with society's ability to cope independently for one or two weeks. In the event of a crisis, even the security organisations need time to become operational. A prepared population gives the police, civil defence and the army this time. A minimum level of personal crisis preparedness is neither particularly expensive nor excessive, but part of every citizen's responsibility.

Questions from the audience

The audience then had the opportunity to put questions to the panellists. The focus was particularly on the further development of total defence, dealing with cognitive warfare and raising public awareness.

When asked about a modern total defence strategy, Droz explained that, despite all existing shortcomings, the current threat situation also presented an opportunity. Unlike before the war in Ukraine, we now have realistic threat scenarios and corresponding arguments at our disposal. It is important to use the time until new resources become available to prepare people mentally and physically: "Et avant, on prépare les têtes, les cœurs et les corps."

Chappuis added that it is not just the army but society as a whole that must be prepared. Whilst various European countries, particularly in the Nordic region, are already preparing their populations for crisis and war situations through information leaflets, discussions in Switzerland regarding the production of such a leaflet have been ongoing for months. The aim is not to stir up fears, but to take responsibility and educate the public.

In the context of cognitive warfare, Chappuis drew particular attention to the targeted dissemination of disinformation and the manipulation of human perception via social media and artificial intelligence: "C'est une guerre invisible avec des armes invisibles et des victimes qui ne sont pas conscientes d'être des victimes." Direct democracy, in particular, offers a particularly large target for such attacks. This makes it all the more important to promote 'intellectual self-defence' – in schools, in the armed forces and in businesses.

Gerber added that the geopolitical dimension of the technological race for artificial intelligence is still scarcely recognised by the general public. Whilst digital applications such as ChatGPT have long been part of everyday life, there is a lack of awareness regarding the strategic objectives with which major powers are promoting their technology industries and striving for supremacy in

the field of artificial intelligence. Gerber expressed doubt that the public was sufficiently prepared for the developments ahead. Just as there are extensive prevention campaigns in the healthcare sector, he argued, targeted awareness-raising campaigns are therefore also needed in the digital sphere.

When asked how the public could be made more aware of the need for crisis preparedness, Pugin expressed cautious optimism. The glass was not only half empty, but also half full: defence issues were increasingly being met with openness and acceptance in both the political and business spheres. Industry, too, must have the courage to make its contribution to security and defence more visible. It is crucial to take the discussion on security beyond the circle of those who are already convinced: “Nous devons toutes et tous avoir le courage de porter ces propos là où les gens sont un peu moins convaincus.”

Droz added that the growing polarisation in both politics and society was making constructive discourse more difficult. The debate was increasingly characterised by attempts to refute the opposing side’s arguments rather than engaging with them seriously. There was a lack of nuance and a reluctance to give other viewpoints any space at all. However, this short-sightedness was also systemic: Changing political leadership has meant that fundamental questions regarding the army’s direction and purpose have been debated anew time and again for decades. It is therefore encouraging that the departmental leadership is now increasingly demanding concrete results rather than further conceptual documents. Whilst the existing system works in principle, it is often too cumbersome to be able to respond to a crisis in a timely manner.

Closing remarks

To conclude the panel discussion, Claude Meier asked the four participants for a brief assessment of what concerned them most in light of the current security situation and what, nevertheless, gave them cause for optimism.

Droz expressed concern about the loss of trust suffered by various security institutions, including the army. However, he said, we must not forget: “L’armée, c’est d’abord la population, c’est d’abord la milice, c’est d’abord ces jeunes femmes et ces jeunes hommes qui s’engagent.” It is precisely his interactions with young members of the armed forces that give him cause for confidence. He recognises in them a growing understanding of the security situation and a willingness to make their own contribution to the country’s security.

Gerber highlighted the well-functioning education system, which transcends social and political divides, and the strong sense of civic duty as particular strengths of Switzerland. This makes him all the more concerned that people in this country sometimes seem almost ashamed to express this sense of civic duty, rather than recognising it as one of their country’s strengths.

Pugin was particularly concerned about the risk of being caught unprepared by a crisis. On the other hand, she was encouraged by Switzerland’s technological, industrial and societal capabilities to respond swiftly to crises. Her own experience of the flood risk on the Rhône had

shown her what forces and resources could be mobilised in the face of an immediately perceptible threat. This made it all the more crucial to raise awareness of existing risks at an early stage.

Chappuis warned against the widespread notion that the future is merely a linear continuation of the present. One must also take into account fundamental technological, societal and security-related upheavals. On the other hand, she finds hope in the resurgent need for a sense of belonging. “Les réseaux sociaux n’ont de social que le nom.” Following a veritable ‘pandemic of loneliness’, she sees a growing willingness to engage with society once again – a development that also benefits the country’s security.

In conclusion, Claude Meier returned once more to the comprehensive understanding of security policy. At its heart lies the preservation of the capacity to act, so that in the event of a crisis, we are able not only to react but also to take active measures. This requires the interplay of all security-related policy areas and instruments.

However, one key element is still given too little consideration in the security policy debate and also in the Security Policy Strategy 2026: people, or rather the population. Meier therefore urged the participants to take the security policy debate into their personal circles as well. For ultimately, as he put it: “C’est ensemble qu’on y arrivera et pas autrement.”