White Paper on Security Policy (June 2016)

Abstract

White Papers on security policy have been published in irregular intervals since 1969. This report, commissioned in March 2014 and published in 2016, focuses on security policy, the future of the Bundeswehr, and sets out directions for the future. This excerpt centers on transnational terrorism, cyber security, and interstate regional conflict.

Source

2.2 Challenges for Germany's Security Policy

Germany's security policy faces a wide variety of new challenges. These differ with regard to the intensity of possible harm, the immediacy of their impact on our security, and the long-term nature of their consequences. Distinctive is their dynamic through reciprocal reinforcement. At the same time, the factor of geographic distance is becoming increasingly irrelevant under the conditions of globalization.

All in all, the spectrum of threats to our security is becoming broader, more diverse, and more unpredictable.

Transnational terrorism

The challenge from transnational terrorism exists worldwide, is not limited to individual states or regions, and is increasing in tendency. Transnationally operating terror organizations and networks profit from processes of state disintegrations, which provide them with room for retreat and in some cases even areas they can control. They use social media and digital communication channels to generate resources, attract followers, spread their propaganda, and plan attacks. They are increasingly capable of attacking targets with cyber capabilities or using chemical, and in the future possibly also biological and radioactive substances in an attack. In addition, they employ criminal methods to finance themselves and to expand their ability to act on a supra-regional basis. It is difficult to track and stop their cash flows.

In addition to al-Qaeda and its regional organizations, whose terror continues to affect Western targets, the terror organization "Islamic State" (IS) has established itself in parts of the Middle East with state-like structures. IS is currently aiming at territorial presence and power projection throughout the Middle East and North Africa to realize its archaically intolerant so-called caliphate. Moreover, it is already carrying its inhuman ideology and its terror to our continent and our society.

Our open and free society, based on respect for diversity, is the enemy and target of this terror.

Terrorist attacks are the most immediate challenge to our security. This risk continues to grow due to the radicalization of sympathizers and the return of violent fighters from crisis and conflict areas (so-called "foreign fighters") to Germany and EU member states, and thus mostly also to the Schengen area, and it is situated at the border between internal and external security.

The effective fight against transnational terrorism therefore requires close national and international, European and transatlantic cooperation. […]

Challenges from the cyber and information space

The safe, secure, and free use of the cyber and information space is an elementary prerequisite for governmental and private action in our globalized world. The growing digitization that permeates all areas of life with its progressive networking of individuals, organizations and states is shaping the opportunities of our present and future in a unique way. At the same time, however, it makes the state, society, and the economy particularly vulnerable to cyberattacks and requires a direct and immediate defense.

Not only the quantity, but above all the quality of the threat has changed noticeably. The technical development from simple viruses to complex, difficult-to-detect attacks (so-called "Advanced Persistent Threats") represents a leap in quality in the threat situation.

Since access to software with high damage potential is comparatively easy and inexpensive, also because of proliferation, the means necessary for cyberattacks are not limited to states. Terrorist groups, criminal organizations, and savvy individuals can also potentially cause considerable damage with little effort. Efforts to create internationally binding regulations or confidence- and security-building measures are thus coming up against narrow limitations.

[…]

Overall, the cyber and information space has thus developed into an international and strategic space for action that is virtually limitless. That space will continue to gain in importance in the future.

Thus, in addition to working on a common understanding about the application of international law, increasing our ability to react and our resilience, as well as preventing and defending against cyber attacks and information operations are indispensable. This also includes coherent and coordinated strategies in the alliance and in the EU.

In view of the problem of attribution that is still inherent in cyberspace, the risk of uncontrolled escalation due to a cyber incident is particularly high. This must be counteracted preventively through confidence-building and conflict-resolving mechanisms.

[…]

Interstate conflicts

The renaissance of classical power politics, which envisages the use also of military means to pursue national interests and is accompanied by considerable armament efforts, increases the risk of violent interstate conflicts - also in Europe and nearby, as the example of Russian action in Ukraine shows.

Increasingly militarily underpinned demands of emerging states to shape their place in the world, against the backdrop of continuing territorial conflicts and the striving for regional supremacy, endanger the stability of the international system - and not only in the European environment. Regional territorial disputes in connection with power projections give South-Eastern and East-Asian states a particular cause for concern. In addition, the risk of escalation of interstate conflicts will increase as nationalist sentiments become more important and are instrumentalized.

In addition, non-state actors, but especially also state actors, are employing methods of hybrid warfare. This includes the use of military means below the threshold of a conventional war. The hybrid approach is aimed at subversively undermining another state. The approach combines very diverse civilian and military means and instruments in such a way that the real aggressive and offensive objectives only become apparent when the elements are seen in their totality.

Hybrid threats require hybrid analysis and defense capabilities. This has a decisive impact on the character and our understanding of national and alliance defense in the 21st century.

Source: excerpt from *Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr*, Berlin, June 2016, pp. 34-38,

Translation: Thomas Dunlap

Recommended Citation: White Paper on Security Policy (June 2016), published in: German History in Documents and Images, <https://germanhistorydocs.org/en/a-new-germany-1990-2023/ghdi:document-5345> [July 15, 2025].