6. Concluding remarks

Re-nationalisation is not an attractive option – while that does not mean it can be ruled out, the pressures emanating from a variety of directions make it at least an unlikely future. Over the last decade, the area of defence policy has become more Europeanised, even though it is surprising to see how much in defence remains national despite the existence of the EU's CSDP. Cooperation on defence through CSDP was almost entirely driven by the voluntary use of bottom-up logic. It did not take the budget crunch to reveal that such cooperation will remain limited and tends to be driven by national preferences that may or may not fit into larger multinational goals. The economic and financial pressures do, however, increase the pressure to make such cooperation more efficient, which would suggest a stronger dimension of top-down direction from the EU level.

Nonetheless, defence policy and the armed forces remain sensitive areas which governments continue to see as touching upon the very essence of their sovereignty. Because there are push and pull factors at work it seems that Europeanisation in form of integration on the EU level will remain a remote possibility. A much more likely development would be that governments chose to pursue project-based cooperation bringing together groups of EU member states for pragmatic, problem-oriented efforts. Cooperation will thus be interest-based, needs-based and flexible. EU-level institutions such as the EDA would have an important role to ensure that such variable geometry pursues broadly aligned goals so that a fragmentation of member state initiatives is prevented.

Hybrid Threats: The Shape of Wars to Come

Sammi Sandawi*

Abstract: Within the last few years, the idiom 'hybrid threats' has become a popular buzzword to describe the complex amalgam of conventional military power combined with irregular tactics, criminal structures and/or asymmetric activities to generate a strategic advantage over traditional armed forces. However, the international debate remains largely limited to new ways of insurgency and counterinsurgency, and is not close to addressing the scale and complexity of the future threat appropriately. The debate tends to focus mostly on operational areas like Lebanon or Afghanistan and too often neglects the domestic domain and the disruptive character that hybrid attacks have on highly complex Western societies. The aim of this article is to broaden the debate on hybrid threats as well as to articulate the parameters of hybrid threats facing Western states – now and in the future.

Keywords: Networked security, hybrid threats, critical infrastructure, non-state actors, new vulnerabilities, irregular warfare

Vernetzte Sicherheit, hybride Bedrohungen, kritische Infrastrukturen, nichtstaatliche Akteure, neue Verwundbarkeiten, irreguläre Kriegführung

1. Introduction

A look at current risks and threats reveals an increasing number of fields of action that are relevant to security policy. This is because the last two decades saw changes on the political, social, technological, economic and military levels that have not only entailed greater freedom for individuals and societies in many countries but have, at the same time, also led to a large number of new risks and vulnerabilities. In this context, it is in particular

- the increased permeability of traditional territorial borders,
- the blurring of the roles of actors in the field of security policy (state/non-state, civil/military, national/international) and
- increased proliferation of defence articles and dual-use goods

that have over the years, promoted the insidious erosion of the state's monopoly of force and have led to an exponential increase in interdependencies between the regions of the world, different policy fields and social entities. This process coincides with the global fusion of knowledge, information and opinion in a virtual real-time/cross-media environment that is extremely vulnerable to manipulation, and society's ever-growing dependence on critical infrastructures (CI) and technologies that are essential for everyday life.

Both in terms of national and international security, these developments have led to a dramatic increase in complexity which creates a number of new vulnerabilities to be exploited by potential (state and non-state) adversaries. In addition to the penetration of direct vulnerabilities, a significantly larger number of indirect effects can be imagined which make themselves felt with delay, indirectly or only in combination

* The author is researcher and political advisor at the Bundeswehr Transformation Centre (Strausberg/Berlin) and the German representative at the NATO-working group on 'Countering Hybrid Threats' (CHT). The views expressed in this article are those of the author and do not represent the views of the German Armed Forces.

with other effects, in particular if use is made of extralegal, intelligence, criminal and/or asymmetrical means.

The particularly threatening effect of attacks on highly networked targets results, on the one hand, from the fact that the intended damage is multiplied by associated measures (1+1=3) and that they trigger cascade effects throughout complex social networks due to which even minor, localized security incidents (e. g. air-traffic related incidents) immediately cause drastic global repercussions in terms of time and money which can hardly be controlled.[1] On the other hand, it must be taken into account that minor individual measures and indirect effects, in particular those that are outside the immediate focus of security policy analysis, may, in most cases, be beyond the range of one's attention. This makes it much more difficult to identify effect patterns and, in the process, detect the attack properly.[2]

Beyond the vulnerabilities readily identifiable from an attacker's perspective, ongoing friction between national authorities and organizations performing security tasks and the still underdeveloped capability to conduct networked risk analysis (including identification of risks and early identification of crises at the interdisciplinary level) may constitute an open flank for potential attackers. This affects liberal societies particularly, due to the way their structures of rule and participation are based on the principle of the separation of powers.

Especially in the event that an adversary employs a hybrid strategy which brings a broad array of attack elements to bear in an orchestrated manner (in part simultaneously, in part consecutively), considerable damage must be anticipated in the light of the vulnerabilities described above as well as low "seismographic" early-warning capabilities. This highlights the necessity to address this topic.

Therefore, in this article, an attempt is made at a first analytical approach to the term "hybrid threat" and the identification of main fields of action and rationales of potential hybrid opponents that result from existing and emerging vulnerabilities. This is followed by a preliminary analysis of national vulnerabilities and structures, which lead to the issue of how present structures enhance and limit the operationalization of counter-strategies.

2. Hybrid Threats: First Findings

2.1 Definition

In order to ensure, for the time being, the broadest possible basis of the analytical process, the term 'hybrid threats' will be defined as any hostile will-imposing approach in which a state or non-state actor employs orchestrated and, in most cases, carefully planned military or non-military means, with special emphasis given to terrorist, criminal, manipulative and/or demoralizing methods. Depending on the particular actor, a hybrid attack may serve political, religious/ideological and economic ends. A hybrid actor may (but does not necessarily have to) be characterized by the following features:

- Pursuit of a strategy aiming at long-term success, generally using indirect means,
- Swift and creative development/adaptation of new tactics and technologies,
- A large portfolio of civil and military instruments,
- Little inclination to self-restriction in terms of observing legal, moral and ethical standards,
- Frequent use of covert tactics with recourse to assets and methods usually employed by intelligence services, including sabotage, terror and contract murder,
- Intensive involvement, use and manipulation of influential mass media,
- A central control level, including a functioning hierarchy, and
- Exploitation of the frequently obscure situation regarding actors and interests in order to conceal own intentions, including the initiation of "side shows" and proxy wars.

Given the above features, hybrid actors and threats cannot be considered as fundamentally new phenomena.[3] What is

CI Sectors

- Energy supply
- Supply (incl. drinking water, health care and emergency medical systems)
- Information and communication technologies
- Transportation (incl. mail services)
- Financial, monetary and insurance systems
- Government authorities, public administration
- Hazardous materials
- Others (media, major research facilities, cultural assets)

Source: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

1 The failed aircraft bombing in Detroit in December 2009 ("underwear bomber") that triggered a worldwide debate about the general introduction of full-body scanners and would involve expenditures in the billions is an example of this.

2 Potential activities include the intrusion into the personal environment of political decision makers, low-threshold acts of sabotage, measures related to economic policy or the manipulation of information.

3 Rudimentary precursors include the "Fifth Column" during the Spanish Civil War in 1936, the "remote-controlled" Sudeten German Free Corps during the Sudeten Crisis of 1938 or the "diversionary troops" employed by the Warsaw Pact in Western countries in the post-war years.

new, however, is the diversity of the vulnerabilities described earlier, making the use of hybrid conflict and attack strategies appear extremely instrumental and promising. In the light of the long-term nature of a hybrid strategy, the lasting effect and implications of a potential hybrid attack and the clandestine and manipulative character of many possible individual measures, the traditional understanding of the following terms becomes blurred:

- Effectors (e.g. due to the large-scale conduct of misinformation campaigns, diplomatic surges, blackmail or the undermining of the reputation of the adversary's decision-makers, extensive use of computer viruses or attacks on computer networks, sabotage of critical infrastructures, currency speculation, imposition of sanctions or the utilization of terrorism and crime),
- Areas of conflict (due to the increasing relevance of confrontations in the information environment including cyberspace and the comprehensive transformation of the economy, the environment and society into arenas for conflict),
- Timeframe of conflict (What defines an attack in times of hybrid threats and when does legitimate or legal defence against such an attack begin? When does a hybrid attack end in the light of clandestine strategies?) and
- Roles of actors (in particular due to the blurring of combatant and non-combatant roles, which also raises the question of who is a legitimate target in the light of hybrid attack strategies).

In summary, the hybrid conflict strategy can be defined as a "negative comprehensive approach". In this context, it must be noted in particular with regard to the identification and rudimentary classification of potential hybrid attackers that the question of the state or non-state character of actors is becoming progressively irrelevant due to the erosion of sovereign powers and the diminishing exclusiveness of military capabilities, whereas the capability to orchestrate a diverse range of effectors and instruments and the capability for the clandestine planning and conduct of operations must be considered vital. In structural terms, especially actors who use comprehensive, homogeneous, hierarchic and trust-, loyalty- or dependency-based networks for command and control, decision making, and communication must be counted among the group of potential hybrid attackers. This is due to the fact that the acquisition and utilization of effectors largely depends on the resolution and unscrupulousness of the actors involved. Thus, the spectrum of potential hybrid actors may range from states (in general under authoritarian rule) to individual large corporations, influential terrorist networks, organized crime groups and insurgent movements to conspiratorial groups acting within government structures.

2.2 Fields of action and instruments of hybrid actors

While the diverse nature of own weaknesses and vulnerabilities as well as the related complexity of potential hybrid attack strategies do not permit the preparation of a comprehensive and complete threat matrix, it is still possible to introduce a somewhat helpful systematic approach to the analysis of hybrid threats and actors by using generic fields of action (that cannot always be clearly delimited from each other) and the related instruments, thus obtaining the following (tentative) list:

- *Military instruments*
  In contrast to a traditional conflict in which the use of (mostly state-controlled) armed forces marks the climax of an ongoing escalation, which was preceded by a sometimes protracted phase of sub-military confrontation, hybrid actors deliberately ignore these highly regulated and, in parts, predictable role concepts and rather seek to mix different styles and forms of attack (with an expected structural preference for sub-military activities), keeping planning and conduct as conspiratorial as possible. Depending on the specific hybrid strategy, military means may be employed at any point of time of the campaign and, for this reason, are not a valid indicator of the actual level to which a hybrid attack has escalated. Since the employment of armed forces can often be expected to attract great international attention on the political and media levels and since, in the process, the existence of a hybrid attack may be disclosed, hybrid actors may rather be somewhat reluctant to overtly use military means or only do so for deception (as a sideshow) or in a covert manner (proxy war).
- *Terrorism*
  Aiming at maximum destruction, catastrophic terrorism must undoubtedly be considered as the main threat of our times. However, the primary objective of terrorist attacks goes beyond the attack itself. Rather, terrorists aim at paralyzing and/or traumatizing the social entity under attack, creating collective fear and provoking (political or military) overreaction. Hybrid attackers may use these effects of mass psychology, which in general can only be minimally controlled, to create diversion or cause social disruption, among other things (see below).
- *Weapons of mass destruction and Weapons of mass effect*
  Nowadays, the use of nuclear, biological or chemical warfare agents no longer marks the peak of escalation in a military confrontation (in which all conventional means have been exhausted) but must be considered an equally apt instrument in the arsenal of hybrid attackers. This is due to the fact that, in addition to the immediate (lethal) damage caused, weapons of mass destruction (WMD) also have considerable psychological effects on the population under attack even if the attack was only attempted or partly successful. Mass panic, disorganized flight and, in extreme cases, the total collapse of public order are possible consequences of such attacks. Furthermore, an NBC attack is often likely to provoke a large-scale military response, which may have to be regarded as part of the hybrid attacker's deeper considerations. In the light of ongoing

technological progress, weapons of mass effect (WME)[4] constitute another distinct set of instruments available to hybrid actors and feature primarily the use of microwave weapons and EMP effects. In the long term, weapons effects designed to manipulate or damage the hormonal system, the DNA or the consciousness of the group under attack are also conceivable.

- *Information operations*
  The information environment of future hybrid attacks plays a special role. The targeted use of misinformation in order to manipulate the adversary's opinion and information spectrum in the short, medium and long term must be understood as 'prima ratio' of any opponent employing hybrid attack strategies. Another aggravating, factor is that national and international mass media nowadays are under a steadily growing pressure in terms of competition, exclusiveness and time (not least due to the emergence of new forms of communication over the internet and social networks). This not only degrades the quality of information but also makes influential information formats more susceptible to manipulation in general.[5] Overall, the deficits addressed above do not just offer potential adversaries a large variety of possibilities to spread short-term collective fear and hysteria among the targeted population but may also distract political decision-makers, who are under pressure to act, from actual/main threats and provoke wrong reactions or overreactions.
- *Criminal activities*
  The active incorporation of criminal methods in a hybrid attack strategy and the use of infrastructure maintained by organized crime groups (e. g. routes for human trafficking and smuggling, weapons caches, money laundry and identity theft capabilities, botnets for denial-of-service (DOS) attacks) offer a variety of possibilities to influence the adversary's actions. They may range from the illegal acquisition of money, weapons and drugs to bribery, corruption and extortion of political decision-makers to political contract murder or the large-scale use of warfare agents (e. g. poisoning of drinking water) as an act of sabotage or WMD measure. Moreover, criminal structures within a state that are sponsored by third parties can be used to undermine the credibility of the political leaders and the law enforcement agencies of that state on the national level and embarrass the government concerned on the international level.
- *Intelligence activities*
  Intelligence services have traditionally employed a hybrid strategy and, when involved in a hybrid campaign managed from a higher control level, their resources, procedures and operational environment make them unique actors that, in addition to the "core task" of intelligence collection and reconnaissance, operate in nearly all the fields of action listed herein. Criminal and/or terrorist activities may also be part of their spectrum of operations, especially in states under authoritarian rule with non-existent or inadequate democratic supervision and control of intelligence activities.
- *Sabotage, manipulation and attacks on computer networks*
  Due to the enormous damage potential, systematic sabotage of facilities and systems must be counted among the preferred aims of hybrid attacks. In this context, the focus is on acts of sabotage that are directed against critical infrastructures and could lead to failure of vital functions of public utility services, thus contributing to a complete collapse of the state within a few days in the event of lasting damage. Disruption of energy, power and water supply is particularly suited to cause eruption of social tensions (looting, insurgencies) and a rapid loss of state control. Considering the current trends in technological progress, acts of sabotage that either directly or indirectly influence the weather (artificial droughts, rainfalls, tornados, etc.) or fundamental biological systems (e. g. by means of genetic engineering of flora and fauna) are also conceivable in the future. In this respect, special attention must also be paid to internet-connected computer networks, which not only form the backbone of information and communication for firms, government agencies and private persons but are in part closely connected with critical infrastructures. Apart from such indirect methods of attack as the targeted manipulation of information (e. g. defamation and smear campaigns via social networks), sabotage (hacking, DDoS attacks) or espionage (trojans, backdoor tools, zero-day exploits), there is also a real danger of direct and harmful interference with public life.
- *Economic, monetary and financial market activities*
  The manipulation of the financial and currency markets must be considered an attractive target of a hybrid strategy in the light of the economic and fiscal fragility of numerous national budgets and/or currencies. Since this field of action is largely non-transparent from the perspective of security policy, targeted activities in this sector are very difficult to detect and counter. The de facto bankruptcy of Iceland due to major currency and stock market speculations by a number of hedge funds illustrates the impact that these processes may have (on security policy). As the large-scale speculation with options on aviation stocks shortly before the attacks of 11 September 2001 illustrates, even minor non-state actors are capable of speculation on the financial markets, not least in order to acquire capital. Apart from stock market activities, the real economy is also vulnerable to hybrid strategies employed by potential attackers. In addition to the "classic" field of industrial espionage and sabotage, this may in particular involve the manipulation of security-relevant procurement processes of the public

4 Definition of WME: "Weapons of mass effect, or WME, are weapons capable of inflicting grave destructive, psychological and/or economic damage [...]. These include chemical, biological, nuclear, radiological, or explosive weapons. While the Task Force recognizes the significant differences in the nature of these weapons, they share many common elements in terms of the requirements for preventing entry into the [homeland]." See U.S. DHS, available at: http://www.dhs.gov/xlibrary/assets/hsac_wme-report_20060110.pdf.

5 The newsrooms of the leading TV stations, print media and web portals, which are increasingly geared to "infotainment", naturally focus on time-critical, polarizing, personalized and visualized news stories and reports since complex backgrounds of the main news story are considered "not suitable" under the conditions of preferably on-site, real-time reporting. Furthermore, the media need less official statements than ever before for the successful presentation of a story since the style of visual presentation and the purposeful placement of interviews with randomly exchangeable "experts" lend sufficient credibility to the news coverage.

sector (armaments, security technology, infrastructure, telecommunications). Hybrid attacks may also lead to the creation of "artificial" demand structures and markets in the public sector (e. g. by initiating a spectacular security incident).

- *Security-relevant research and development*
  In nearly all fields of scientific research one can foresee or at least vaguely imagine developments that may revolutionize the interaction between state and society, the military and conflict, and humans and machines. This applies most obviously to the fields of information and communication technology, biotechnology, medical technology (including human genetics), robotics, neurotechnology, nanotechnology, materials research and energy-related research. To a large extent, however, many future developments may also be used in conflicts, since those actors who are leading the respective fields of research possess a potentially decisive edge.
- *Political and diplomatic activities*
  States employing a hybrid attack strategy have at their disposal a wide range of possibilities to exert influence, since they are integrated into the international system, politico-diplomatic networks and possible alliance structures. The combination of media manipulation and diplomatic surges (imposing sanctions, appealing to international bodies, etc.) may be particularly effective in this respect. In this context, hybrid attackers may also resort to overt or covert support of forces opposing an adversary.
- *Political subversion and manipulation of society*
  As open-minded, urbanized, ethno-culturally diverse, highly networked, heterogeneous and post-heroic as it is, liberal democracy, more than any other social order, must be considered susceptible to strategies of social division and subversion and offers hybrid attackers a wide range of possibilities to employ long-term subversion strategies. In this context, the Achilles heel of liberal democracy is not the social order as such or existing liberty rights and defensive rights (in contrast to authoritarian forms of rule) but – nearly inevitable in pluralistic, globalized and highly individualized Western-style societies – the erosion of the "social glue", which elsewhere exists in the form of ethnic, national or ideological societal foundations and the absence of which may be exploited by external hostile actors. In addition to the aforementioned means of terrorism and sabotage, this may especially involve activities related to political subversion: from systematic discrediting of political and social elites (e. g. through diversion and propaganda) to covert support of opposition forces to fuelling social, ethnic and/or religious and ideological resentments and conflicts or the promotion of crime, drug addiction and subversive subculture.

In addition to the fields of action mentioned herein, a differentiation must also be made between direct and indirect effects, and possible potentiating and cascade effects taken into consideration:

- *Indirect effects*
  The effectiveness of a hybrid attack increases, along with the concealment of hostile activities and the related chain of effects. For this reason, it must be assumed that hybrid planning does not attempt to directly influence a visible process but rather aims at causing the intended primary effect, employing hardly detectable methods and activities, while staying out of range of the adversary's intelligence assets. In this context, assassinating one of the adversary's decision-makers may not just prove difficult in the light of close protection but inevitably raises critical questions about the political background of the act, which might prove counterproductive in a strategic timeframe.[6] Instead, disruptive interference of target persons' personal life, including the resulting psychological effects or the instigation of tragic chains of events and accidents, causes much less suspicion.
- *Potentiating effects*
  Through the smart combination of different effects, the overall effect of hybrid campaigns may be potentiated. The disruption of the communication and energy infrastructure shortly after a major terrorist attack is an example of this. Being cut off from the flow of information, the feeling of being victimized oneself by an (ongoing) attack, along with complete disorientation as to the time, place and dimension of the attack, may cause mechanisms of mass psychology to take effect ("escalation of the irrational") and result in collective panic in next to no time.
- *Cascade effects*
  While cascade effects triggered by hybrid attacks may certainly be potentiating, the specific dynamics of these effects require classification as a separate category. Especially highly-networked complementary systems without sufficient redundancies are susceptible to attackers who use cascade effects in an effort to cause the complete system or at least large parts thereof to fail by way of the (easily possible) elimination of minor subsystems. Local power outages that can lead to a large-scale blackout due to increasing power grid overloads and/or shutdowns are an example of this.[7] The prolonged disruption of power-dependent systems and end devices, which may plunge a society into a crisis, must be considered the nth level of the damaging cascade.

3. Vulnerabilities and Counter-Strategies

3.1 Internal frictions and resistances

In addition to new vulnerabilities, the developments of the last decades have also brought about new rationales and targets, some of which substantially differ from the traditional understanding of conflict and the way conflicts used to be

6 Current examples of the strategic setback of political murder conspiracies are in particular the murder of Zoran Djindjic (2003), which contributed to strengthening democratic forces in Serbia, and the murder of former Lebanese prime minister Rafiq al-Hariri (2006), as a result of which Syria was forced to withdraw from Lebanon.

7 Large-scale power outages in the US and Canada (August 2003) and in Western and Southern Europe (November 2006) are examples of this.

fought. Western societies in particular feature vulnerabilities that expose them to potential attackers (as described above) and that therefore deserve careful strategic consideration.

Nevertheless, security policy debates often fall short of realizing the potential of "new" types of threat and attack and the possibilities that may arise from combining military and non-military instruments. In this respect, it is worth noting that force and defence planning often draws on experiences from the last conflict that was fought (or observed). An adversary may gain a decisive strategic advantage by systematically identifying, analyzing, operationalizing and exploiting these planning gaps.

On this basis, it is possible to identify a number of deficiencies of security structures with regard to hybrid threats which may have considerable negative impact on national security.

- The primarily responsive nature of security and defence policy,
- The fact that the approach taken by governmental security agencies predominantly focuses on the respective departments and areas of responsibility, with only selective networking or integration,
- The severe lack of "strategic imagination" on the part of political and military decision-makers, including relevant staff and administrative structures,
- Insufficient future orientation of security policy analysis and advice,
- The fact that development and procurement cycles of (defence) technology for the armed forces and security agencies are often protracted, including slow progress during parts of the roll-out and implementation phase, and
- The vulnerability to surprise attacks resulting from the above-mentioned processes.

Besides a lack of careful analysis and foresight in the field of security policy, there has been neither a timely legal response to these changing conditions, nor have these been properly evaluated and clarified, as would be required by an anticipatory and structurally adaptive national security policy. Especially the redefinition of the use of force pursuant to international law, the legal understanding of an attack and of the actors involved in a conflict (combatants, civilian population) has been overdue for years.

Even the awareness that hybrid attacks are a potential threat does not necessarily give reason to expect that the actors responsible for early analysis and countermeasures will readily embark on a harmonized concept for preventive security. Limited resources, structural frictions on the departmental level and conflicts over jurisdiction almost inevitably affect the coherence of cooperation. In Germany for instance, controversies about the domestic employment of military forces, the deployment of police officers abroad or the separation of law enforcement and intelligence agencies as laid down in the constitution are only the most prominent examples of problems surrounding the networked security. Furthermore, the most important aspect of early and effective counter-activities against hostile hybrid campaigns, namely the immediate and lossless sharing of information and intelligence between different agencies, government bodies as well as (if appropriate) the private sector (companies, think tanks, NGOs), remains the "Achilles heel" of a comprehensive approach in the field of security.

3.2 Approaches for a counter-strategy

There is no silver bullet in countering hybrid threats in general, and preventive measures cannot be put into practice in all areas potentially relevant to security. Thus, only carefully structured knowledge about potential hostile approaches may be considered decisive for preventive, pre-emptive and responsive measures.

Identifying own (new) vulnerabilities and resulting (new) strategies, means and methods of potential adversaries is the analytical starting point for counter-strategy considerations with regard to hybrid threats. A national and/or alliance-wide system-of-systems analysis (SOSA) using (G)PMESII[8] can be used as an initial methodological approach for identifying potential threats posed by hybrid attackers. The same applies to the increased use of "red teams" and strategic future analysis. At the same time, it must be noted that hybrid threats by nature cannot be fully analyzed and predicted, a circumstance that is reflected in current U.S. debate: "it may be prudent for DoD to describe and not define its newly appreciated hybrid environment, its myriad hybrid challenges, and its likeliest (and most important) hybrid responses to both. What is critical to increased defense appreciation for the operating environment is not 'one time' precision in defining hybrid warfare but instead perpetuation of an active dialogue on a new and expanding universe of complex defense-relevant challenges."[9]

Coordinating activities related to networked security and overcoming partially significant problems regarding horizontal coordination between national authorities and organizations performing security tasks on the one hand and the lack of vertical networking between national and international structures on the other hand are the principal starting points for strategic countermeasures. There is also a need for resolute political action which may, among other things, require intensive preparation on the administrative side and a rise in awareness levels. The still underdeveloped capability to conduct networked risk analysis (including identification of risks and early identification of crises at the interdisciplinary level) may in particular constitute an open flank for potential attackers. Still, it must be admitted that not even the best possible analysis can provide complete protection against the effects of strategic surprise. In the light of the described threat, the comprehensiveness of own (national and/or alliance-wide) reconnaissance systems is to be considered fundamental to one's own ability to act and indeed places the implementation of the networked-security principle at the centre of preventive

8 The abbreviation (G)PMESII stands for geographical, political, military, economic, social, infrastructure & information and describes an analysis model used to demonstrate the complex interaction of effects in the field of security policy.

9 Nathan Freier, "Hybrid Threats and Challenges: Describe... Don't Define," in *Small Wars Journal,* 2009, available at: http://smallwarsjournal.com/blog/journal/docs-temp/343-freier.pdf.

and responsive measures. The fields of action to be included in this process involve

- awareness (strategic analysis and anticipation, raising political awareness),
- preparedness ("seismographs" and emergency plans, raising the population's awareness),
- active countering (addressing weak points and eliminating vulnerabilities, networking security structures).

Based on a broader understanding of a counter-strategy, long-term efforts must aim at using opportunities created by hybrid approaches and strategies for national campaign planning and employing networked approaches when actively pursuing and advancing own interests in the field of security policy.

At the same time the potential comprehensiveness and impact of a future campaign also emphasize that countering hybrid threats cannot be an isolated national effort. While there is an obvious need for a stronger nexus between national aspects of internal and external security and the focus of the national security debate should progressively shift away from operational areas like Afghanistan and Iraq and more towards existing (and future) domestic vulnerabilities, the international dimension must not be overlooked. Indeed, the growing global complexity and interdependency positively forces Western states to the widest possible cooperation and coordination in the field of security. This includes especially a better and pro-active information exchange on potential and rising threats and possible hybrid actors, the development of common (European/transatlantic) counter-strategies, early warning systems and contingency plans as well as joint interdisciplinary efforts in the field of future technology assessment.

Space and Security – Challenges for Europe

Nina-Louisa Remuss*

Abstract: The basic idea behind the European integration process was to establish peace and security through economic integration. Once a common understanding of "peace" and "security" had been established, the necessary instruments for providing security had to be found. Among these instruments are space applications, which are increasingly relied upon in Europe and which have come to contribute to the development of a certain European role and identity among the other actors. Europe is building up its own capacities and related governance structure. This article is meant to provide the introductive facts by outlining the current developments in the context of space and security and highlights the challenges for Europe.

Keywords: Space security, code of conduct, Space Situational Awareness, Responsive Space, transtatlantic cooperation
Weltraumsicherheit, Verhaltenskodex, Space Situational Awareness, Responsive Space, transatlantische Kooperation

1. Space and Security vs. Space Security in the post-Cold War era

In the post-Cold War realm one can observe two changes when speaking about space and security. The first is more generally linked to a change in the definition of security as a result of the changing nature of threats to security, from traditional state-to-state territorial attacks to non-traditional so-called functional threats coming from non-state actors sometimes even from within the own state's boundaries.[1] It is now commonly distinguished between external and internal security. Given the need for innovative tools, space applications are increasingly used as instruments in the provision of security.

The second change is connected to space systems in particular. With the end of the Cold War, the bi-polar hegemony of the two superpowers ended and more and more states enter space, making outer space an ever more contested environment. At the same time the dependence on space applications for the functioning of society increases. Satellites provide telephony, real time broadcasting (e.g. Olympics, world cup coverage), video conferencing, faster, more secure banking and financial transactions. They are also bridging the regional and digital divide by providing broadband internet access and allow, for example, for e-learning in rural areas. European Union external security missions such as the EU Military Crisis Management Operations EUFOR Chad / RCA rely (and depend) on satellite communication for secure communications between the Operations Headquarters (OHQ) and field deployments and on satellite imagery for mapping in support of the mission. Research is also conducted in relying on space applications for internal security missions such as border- and transport security as well as for critical infrastructure protection.

* Nina-Louisa Remuss holds a M. Litt. in International Security Studies from the University of St. Andrews and a B.A. in European Studies from the University of Maastricht. She is Associate Fellow, based in Berlin, at the European Space Policy Institute (ESPI) in Vienna, Austria.

1 For a detailed account on the development of the concept of security consider Sundelius, Bengt. "Disruption – Functional Security for the EU." Disasters, Diseases, Disruptions: A new D-drive for the EU. Chaillot Paper No. 83. Ed. Antonio Missiroli. Paris: Institute for Security Studies, 2005; Varwick, Johannes and Woyke, Wichard. NATO 2000. Transatlantische Sicherheit im Wandel. Augsburg: Leske + Budrich, 1999. 30-1; Varwick, Johannes and Woyke, Wichard. Die Zukunft der NATO. Transatlantische Sicherheit im Wandel. 2nd Edition. Augsburg: Leske + Budrich, 2000. 127.