Forward Resilience in the Age of Hybrid Threats: The Role of European Intelligence

Björn Fägersten

Introduction

Discussions on hybrid warfare and hybrid threats have dominated the European security debate in recent years.[1] Hybrid threats usually refer to a coordinated mixture of military and non-military and covert and overt means in order to reach specified objectives. As such hybrid tactics is about increasing uncertainty in a conflict situation, blurring the line between war and peace and between aggressor and victim. Intelligence work is one important tool in order to reduce the uncertainty that characterizes security policy in general and hybrid threats in particular. How can national and international means be employed to counter hybrid threats? What are the main vulnerabilities of European states and the resilience needed to withstand hybrid threats and tactics?

Hybrid Threats and Intelligence

The European Union (EU) increasingly functions as a security provider. While article 4(2) of the Treaty on the European Union makes clear that national security is the prerogative of the member states, other measures and policies in the realm of security have been added incrementally to the Union's remit. With activities in the field of *safety, internal security, external crisis management,* and *civil protection*, the Union is effectively closing in on the vague concept of *national security*.

When national governments, and increasingly the European Union, make decisions relating to security they do so under conditions of uncertainty – who is the enemy, what course of action is most suitable and what long term effects can be envisioned, etc. In an age of hybrid war and threats, this uncertainty is bound to increase. One key element in countering hybrid threats is therefore to reduce the level of uncertainty. This can be facilitated by independent media, strong academia, civil society etc. But governments have other means as well as they can employ intelligence[2] agencies to reduce uncertainty in areas where other knowledge producing functions are insufficient.

This chapter discusses how intelligence efforts – national as well as international – can be employed to build resilience in the face of hybrid threats. To grasp the role of intelligence as a

[1] I would like to thank Costan Barzanje and Denise Peters for excellent research assistance in preparation of this chapter.

[2] Intelligence agencies can be distinguished from these other functions in regards to *security* and *secrecy*. The first implies that intelligence agencies are foremost interested in questions that pertain to security – be it human, national or international. The second – secrecy – has a dual meaning as it applies to the often concealed and protected nature of the sought information as well as the stealthy manner in which intelligence organizations tries to acquire this information.

tool, I will first look at the vulnerabilities of European states and the resilience needed to withstand hybrid threats and tactics.

Vulnerability and Forward Resilience

Modern Western states have specific societal vulnerabilities in the face of hybrid threats.[3] Indeed, one can argue that within this larger group, the northern states with open societies, trade-dependent economies and a relative lack of domestic strategic resources stand out among Western societies.[4]

A first area of vulnerability is the political cohesion within vital cooperation forums. For most European countries this would constitute a mix between the European Union, NATO and the OSCE. Political cohesion within these bodies, and especially the EU and NATO, is a precondition for the management of common political and security problems. The risk of decreased decision-making capacity within these bodies due to hybrid tactics – by, for example, supporting fringe parties, co-opting weak national leaders or dividing countries by modes of negotiation – constitutes a considerable vulnerability.[5]

A second area would be control of territory and critical infrastructure. Ukraine, and the annexation of the Ukrainian region of Crimea, illustrates the territorial threat of hybrid tactics. The abduction and detention of an Estonian security official on Estonian territory proves that even EU members encounter threats on, and ultimately to, their territory. Cyberattacks on critical infrastructure such as Sweden's air control systems or Germany's parliament proves that vulnerabilities regarding state control are not limited to physical territory.

Third, Western societies are vulnerable in the area of societal cohesion. Religious and ideological radicalization, ethnic conflict and minority conflicts can be instigated by external actors in a hybrid conflict situation either through support of specific groups or by efforts to fuel conflicts among groups. Last, and as indicated initially, Western societies are hugely dependent on a variety of global flows. Ever more interdependent, European states – and those in the north in particular – need to manage flows of energy, data and capital and secure the access points to these flows.[6]

The ability of states to resist and recover from disturbances regarding the vulnerabilities outlined above is referred to as resilience in this chapter. As such, resilience is a perishable shock-absorbing capacity at the national level. However, growing interdependencies means that resilience is not merely a national affair, and neither is it confined to current interdependencies - others may emerge over time. The term *forward resilience* has been suggested to cover these

[3] For an overview, see Claudia Major and Christian Mölling, *A Hybrid Security Policy for Europe*. SWP Comments, 2015/C (22), 2015.

[4] See for example Mika Aaltola, ed., (2014). "Forward Resilience and Networked Capabilities: Finland's Softer Power Tools in the Wake of Ukraine," in Daniel S. Hamilton, Andras Simonyi, Debra L. Cagan, eds., *Advancing U.S.-Nordic-Baltic Security Cooperation*. Washington, DC: Center for Transatlantic Relations, 2014, available at: https://oaklandstreetpublishing.com/samples/Advancing_Nordic_Baltic_final.pdf [Accessed 23 Nov. 2016].

[5] Major and Mölling, op. cit.

[6] Aaltola, op. cit.

spatial and temporal extensions of the concept.[7] The spatial dimension relates to the fact that just as with sovereignty, resilience is today shared over borders. All of the vulnerabilities suggested above have clear transboundary logics. For European political cohesion and flow security it is rather obvious, as they are transnational by nature. But territorial control is also shared in Europe today, as the migration crisis has illustrated. Critical infrastructures are interwoven where, for example, the resilience of one state's air control capacity is a security concern for all. And societal cohesion is linked as well, as many of radical elements cooperate and operate across borders. The temporal dimension relates to the fact that the threats pinpointing the above vulnerabilities can be addressed along a wide continuum ranging from forecasting and trend analysis via current operations to post-event analysis and adaptation.

Hybrid Threats and Forward Resilience in EU Strategy

The transboundary nature of the hybrid threats outlined above has increasingly been addressed in the European Union by propositioning conjoint measures to foster resilience. To this end, the European Commission and the High Representative adopted a Joint Framework on countering hybrid threats[8] in April 2016. The Framework lists four areas along with an action plan of 22 measures where development at both EU and member state level should be made in order counter hybrid threats. The four main areas in the framework are 1) raising awareness, 2) building resilience, 3) preventing, responding, and recovering from crisis 4) stepping up cooperation with NATO and other organizations. Many of the suggested actions are to be included in projects already in force or undergoing implementation. The actions also call for member state cooperation and action since the Framework applies in context of the Common Foreign and Security Policy (CFSP), and thus rely on competence that lies within the national sphere. Some of the measures that have already been taken in a response to the Framework include the introduction of a Hybrid Fusion Cell, the launch of a contractual Public-Private Partnership (cPPP) for cybersecurity, the signing of a code of conduct with Facebook, Twitter, YouTube and Microsoft to prevent radicalization, and the signing of a joint declaration between the EU and NATO calling for further cooperation on countering hybrid threats.[9]

In June 2016 the EU also launched its new Global Strategy for the European Union's Foreign and Security policy (EUGS)[10]. In the EUGS, the EU elaborates an integrated approach linking internal resilience with EU's external actions, noting that "security at home depends on peace beyond our borders," and accordingly places geographical priority from Central Asia to Central Africa. Given the current turbulence in the region, ranging from the prevailing Russian threat

[7] For a discussion, see the Preface to this study by Daniel S. Hamilton, http://transatlanticrelations.org/wp-content/uploads/2016/12/resilience-forward-book-hamilton-final.pdf

[8] European Commission, *Joint Framework on countering hybrid threats*. Brussels: European Union, April 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 [Accessed November 23, 2016].

[9] The Council of the European Union, *CFSP Report - Our priorities in 2016* (Document: 13026/16) General Secretariat of the Council: Brussels, 2016, available at http://data.consilium.europa.eu/doc/document/ST-13026-2016-INIT/en/pdf [Accessed November 23, 2016].

[10] European Union, *A Global Strategy for the European Union's Foreign and Security Policy*. Brussels: European Union, 2016, https://eeas.europa.eu/top_stories/pdf/eugs_review_web.pdf [Accessed November 23, 2016].

to terrorism to refugee flows, the Strategy emphasizes that one of the key strategic priorities of the EU is to invest in state and societal resilience by strengthening the capacity of the EU and its neighbors to withstand internal and external crisis. The EUGS Implementation Plan,[11] released on November 14, 2016, presents implementation proposals to the EUGS in the area of security and defense. Both the EUGS and its Implementation Plan describe a Europe that needs to adapt and update its take on security. In this endeavor, the countering of hybrid threats play an important role, and much effort is being put into increasing expertise and assistance to partners through strategic communication and better cyber security along with the protection of networks, critical infrastructure, and energy security. The Plan proposes resilience as a method to counter hybrid threats and stresses the need for common analysis of crisis and coherent and comprehensive joined-up action.

Concerning resilience, the EU is developing an equal amount of strategies in terms of strengthening the ability of its member states and partners to handle crises, and to efforts to prevent such crises from happening. For that reason the concept of resilience was included in the Joint Framework previously mentioned. It was also addressed in the EUGS and the ensuing Implementation Plan. The means of implementation for enhancing resilience are proposed as strategic operational actions aimed at increasing cooperation in security by establishing mechanisms for exchange of information and by coordinating actions to deliver strategic communication, address strategic vulnerabilities in strategic and critical sectors such as cybersecurity and critical infrastructures, and by preparing for coordinated responses by defining effective procedures to follow.

These strategic actions are prevalent, for instance, in EU ambitions to further develop its strategic partnerships. Here NATO, the UN, OSCE and the African Union are of great importance. For example, efforts to implement the jointly agreed priority areas for strengthening the UN-EU Strategic Partnership on Peacekeeping and Crisis Management will be made. The EU and the OSCE will also enhance their common work on operational capabilities, promotion of stability, inviolability of borders, adherence to human rights and fundamental freedoms, rule of law, media freedom, and fair democratic elections. In addition, the next EU-Africa Summit will offer a potential opportunity to reconsider the Peace and Security Partnership between the two sister organizations in light of the renewed approach to capacity building in the field of security. Furthermore, special consideration is to be given to the Common Security and Defense Policy's (CSDP) partnerships with partner countries that share EU values and are able and willing to contribute to CSDP missions and operations to promote resilience in the EU's surrounding regions. The importance of security in the Review of the European Neighborhood Policy (ENP)[12] and the forthcoming initiative on resilience-building as part of the broader implementation of the EUGS should also be taken into account.

[11] European Commission, *Implementation Plan on Security and Defence.* Brussels: European Union, 2016, https://eeas.europa.eu/sites/eeas/files/eugs_implementation_plan_st14392.en16_0.pdf. Accessed November 23, 2016.

[12] European Commission, *Joint Communication; Review of the European Neighbourhood Policy.* Brussels: European Union, 2015, https://eeas.europa.eu/enp/documents/2015/151118_joint-communication_review-of-the-enp_en.pdf. Accessed 23 November 23, 2016.

Moreover, the EU looks into enabling a more rapid response in the event of a crisis. Accordingly, it seeks to improve the usability and deployability of the EU's rapid response toolbox where synergies with other high readiness initiatives, notably within NATO, will be made along with large-scale and regular 'live' civil and military exercises and the development of a rapidly available common pool of strategic lift assets for the deployment of EU Battlegroups.

In relation to the resilience approach, above all, two questions have been heralded: 1) what does resilience and resilience-building actually mean; and 2) what are the implications of the rise and application of the resilience approach in EU policies.[13] However unclear what the concept of resilience entails and how it is to be applied, what is clear is that it has come to pose a challenge as a concept in its own right. Wolfgang Wagner and Rosanne Anholt concede that the dispersion of resilience in a range of fields has led to the confusion of what it supposed to mean. They do however acknowledge that the reason for its omnipresence in the EUGS is that it relates to a broad range of fields and referent objects, for example, externally it relates to the enhancement of resilience of states and societies in the EU's broad neighborhood, and internally by strengthening critical infrastructure, networks and services.[14]

Ana Juncos acknowledges the introduction of resilience in the EUGS's "principled pragmatism" approach as a move towards a more pragmatic foreign policy that allows for the EU to take into account both the need for cooperation and at the same time face competition on the part of other international powers.[15] However, she finds the adding of "principled" to the pragmatic turn as problematic in its continued adherence to liberal logic and achievement of universal values."[16] As such, the EU is caught between two different logics -- the old neo-liberal stance that considers threats, defense geopolitics and liberal intervention, and the new logic of risk, resilience, complexity and capacity-building. The principled pragmatism approach, she argues, will not only expose the EU to charges of arbitrariness and inconsistency in its external actions, it also risks undermining the principles it stands for by not corresponding to its normative standards.[17] In contrast, Wagner and Anholt appreciate resilience as a practical middle ground between an "over-ambitious liberal peace-building and under-ambitious objective of stability." Whereas the practicality of liberal peace poses an impractical endeavour, the adoption of stability as a new paradigm would stand in dire contrast to the idea of Europe as a normative power with the aim of promoting democracy, rule of law and human rights. Wagner and Anholt argue, however, that resilience, with its positive objective of focusing on solutions rather than on problems along with its disposition for practicality, has posed as the

[13] Ana Juncos, "Resilience as the new EU foreign policy paradigm: a pragmatist turn?" *European Security*, online, 2016. Wolfgang Wagner and Rosanne Anholt, "Resilience as the EU Global Strategy's new leitmotif: pragmatic, problematic or promising?" *Contemporary Security Policy*, 37(3), 2016, pp.414-430. F. de Weijer, *Resilience: A Trojan Horse for a New Way of Thinking?* ECDPM Discussion Paper(139), (2013).
[14] Wagner and Anholt, op. cit., p.415.
[15] Juncos, op. cit., pp. 8, 11.
[16] Ibid. p. 11.
[17] Ibid. p. 13.

perfect middle ground.[18] Furthermore, they argue that resilience is far more cautious than liberal optimism and allows for an understanding of crisis as inevitable, if not imminent, and as such offers a means to balance expectations of what the EU can accomplish.[19]

However the concept of resilience may develop and be used in the EU context, the strategic ambition – as put forth in official documents – sseems to recognize the need to prioritize a mutual approach and combined effort to enhance resilience by anticipating crisis through risk assessment, focus on prevention and preparedness, and enhanced swift response and recovery from crisis.

Mapping the Roles of Intelligence

Having first discussed the hybrid threat and the vulnerability states face and second the EUs strategic ambitions in the resilience field, what is the role of intelligence in building forward resilience? In this section I will suggest four generic functions that intelligence services can perform in the face of hybrid threats.

Identify Vulnerabilities at Home and Abroad

In line with the overarching function of intelligence – to reduce uncertainty – intelligence agencies and security services have a key role in identifying the vulnerabilities within the societies and organizations they are tasked to protect. This could imply analysis of decision-making capacity within international security organizations, identify what parts of a country’s critical infrastructure is most vulnerable and most likely to be targeted, follow the work and organization of radical political elements, and make assessments of flow dependency and security.

These tasks could be performed with a short time horizon in the form of a ‘stress test’ of core societal functions or by long-term scenario analysis, i.e. spanning the temporal dimension of forward resilience. Likewise, analysis of other countries' vulnerabilities is common within intelligence work, either as collaborative effort or without cooperation from the target country.

Address such Vulnerabilities at Home and Abroad

In many cases, intelligence agencies also have a role in the subsequent phase of addressing identified vulnerabilities. Tasks could be to shore up decision-making procedures, staging civil and military crisis exercises, secure access points that connect countries to global flows etc. This can be done well in advance (long-term training) or with a focus on immediate capacity improvement. Vulnerabilities can also be addressed abroad, for example through benchmarking and security sector reform. A good example is the way Western intelligence and security services helped reform their equivalents in eastern Europe prior to NATO and EU accession. This work was carried out bilaterally as well as multilaterally in forums such as Club de Bern and the Counter- Terrorism Group. By addressing vulnerabilities within the new members'

[18] Wagner and Anholt, op. cit., pp. 413, 417, 418.
[19] Ibid., p. 424.

security sector, security was improved both ‘home’ and ‘abroad’ and conditions for future security cooperation was met.

Warn Against and Monitor Hybrid Threats

Warning and monitoring is a fundamental task of intelligence and security services and relates to all of the vulnerabilities above. As in the tasks above, warning and monitoring of threats can be done nationally, in cooperation with partners or even on behalf of unknowing partners. It could also be performed with a long time horizon as horizon scanning or early warning or as more immediate situational awareness. Collaborative warning and monitoring requires a shared understanding of vulnerabilities as well as perceptions of threats.

Counter Hybrid Tactics

Finally, intelligence and security services have a role in countering hybrid tactics as they take place. This could imply security services averting sabotage or intrusion of “little green men” or it could be intelligence agencies with offensive cyber capabilities that thwart ongoing attacks. While this is task that is played out in real time, it can be practiced and prepared, also in cooperation with partners.

Fact Box – EU Intelligence Structures

INTCEN – EU intelligence and situation centre: The main hub for intelligence analysis within the EU. Situated within the External Action Service, INTCEN produces reports and briefings based on contributions from the member states’ intelligence services, material from other EU bodies and opens sources. INTCEN mainly provides intelligence support to the CFSP but also covers issues of an internal character such as counterterrorism.

INTDIR – Intelligence division of the EU military staff: Works closely with INTCEN but is solemnly devoted to military affairs. It reports to various bodies within the European External Action Service (EEAS) but particularly to the Military Committee. INTDIR often produces joint reports with INTCEN under a work format called Single Intelligence Analysis Capacity (SIAC).

EUROPOL – European Police Office: A hub for exchange and analysis of criminal intelligence. Information originates from member states, open sources and third parties such as international organisations and countries beyond the EU.

CTG – Counter Terrorism Group: Consists of EU member states together with Norway and Switzerland and is positioned outside of EU structures, even though it provides analysis to various EU decision-making bodies.

FRONTEX – The European border management agency: Functions as both a consumer and a producer of intelligence. Produces risk assessments on data received from national border authorities and other sources.

SATCEN – The EU Satellite Centre: Produces geospatial and imagery intelligence products on behalf of the High Representative of the Union for Foreign Affairs and Security Policy (HRVP). The primary sources of satellite data are commercial providers but SatCen has some access to national resources as well.

Challenges of European Intelligence Cooperation

The section above outlined the roles of intelligence in building forward resilience to hybrid threats. Both the temporal and spatial dimensions of forward resilience demands functioning international cooperation in the intelligence field. In Europe, such cooperation has developed considerably over the last 15 years and now covers law-enforcement intelligence, security service cooperation on terrorism and internal security, as well as civil/military intelligence cooperation in support of foreign and security policy.[20] While cooperation has developed extensively – see the fact box – challenges prevail. Four challenges stand out when considering cooperation against hybrid threats.

Diverging Member State Interests

Countries share intelligence, or establish joint intelligence functions, if they believe this furthers their interests.[21] Economics of scale and the need to support common policy objectives often offer a rationale for cooperation. But other interests balance these benefits, such as the risk of exposing one's sources and methods, the risk of being deceived through cooperation or a concern for national autonomy. In sum, even in relation to hybrid threats and shared resilience, it has to be acknowledged that regardless of the sound economy of sharing and cooperating as well as an overall interest in furthering a specific joint policy or instrument, cooperating states will in some instances deem it counter to their interests to take part in common intelligence work.

Bureaucratic Resistance

Not only member states have interests, so do their intelligence professionals, and at times they differ considerably.[22] The reasons may vary. Cooperation may be impeded by different organizational cultures in the concerned countries. Equally important, professional cultures differ among police forces, security services and intelligence agencies, which is challenging in areas when these forces need to join up, such as in the counter-terrorism field. Bureaucratic self-interest plays a part as well, for example when new cooperative arrangements threaten investments in long-time personal networks. The sum of these bureaucratic factors implies that governments' ambitions do not always translate into reality. The short history of multilateral intelligence cooperation in Europe provides plenty of examples. The ambition to put Europol at the center of the fight against terrorism, repeated after most terrorist attacks on European soil, has for example been severely obstructed by the fact that national security and intelligence agencies have not been willing to strengthen their cooperation with a police body.

Lack of Cross-Sectoral Cooperation

One challenge of a more specific nature is the cross-sectoral demand that hybrid threats put on intelligence work. The fact that hybrid tactics spans several domains (civil society, cyber, the military realm, etc.) means that intelligence-sharing to counter these tactics must cover a broad

[20] For a recent overview see Björn Fägersten, *Intelligence and decision-making within the Common Foreign and Security Policy*. Sieps, [online] 2015(22epa), 2015, available at http://www.sieps.se/sites/default/files/2015_22epa_eng.pdf, accessed November 23, 2016.

[21] Björn Fägersten, *For EU eyes only? Intelligence and European security*. EUISS, [online] (8), 2015, available at: http://www.iss.europa.eu/publications/detail/article/for-eu-eyes-only-intelligence-and-european-security/, accessed November 23, 2016.

[22] Ibid.

range of actors and organizations. This is usually difficult enough to accomplish at the national level, and even more so on an international level.

Temporal Mismatch

An adjacent challenge is that of differing temporal perspectives in relation to hybrid threats. Looking at the information flows in support of EU foreign policy, there is, or at least there has been, a mismatch between the temporal dimensions of support and demand. Until now, intelligence support has been strongest in the short- to medium-term perspective, looking at issues three months to two years ahead. Current intelligence has been of a non-clandestine nature, essentially coverage of news reports and other open sources in real time. This is in contrast to the policy cycle of the EU's foreign policy, where most effort goes into either long-term structural reform programs or the deployment of civil and military missions where open source intelligence is not enough.[23]

Conclusions and Policy Recommendations

This chapter has discussed the hybrid threats that befall European countries and the increased levels of uncertainty they entail. One of the ways to respond to these threats is to build resilience at home and in partner countries and the strategic ambitions of the European Union in this field have thus been analyzed. Finally, the roles of national and international intelligence in supporting resilience have been outlined, as have the challenges that beset international intelligence cooperation. Based on this analysis, what could then be done in order to allow for improved intelligence support to resilience building at home and abroad?

First, one important contribution would be to establish genuine multilateral intelligence training. Many of the challenges to international intelligence cooperation and information sharing have roots in insufficient levels of trust and lack of knowledge of the bureaucratic and cultural procedures in partner countries and agencies. These often deep-rooted barriers to cooperation are difficult to circumvent by intuitional novelties or executive orders. They can, however, be mitigated by training, whereby individual officials learn the habit of multilateral intelligence. The EU IntCen, which now hosts the new hybrid fusion cell, already runs training modules for newly seconded analysts. This could rather easily be scaled up and offered to all new national recruits, not only those manning EU intelligence positions, but also to non-intelligence officers within the EU bureaucracy (such as analysts working in the external EU delegations), to NATO officials in order to familiarize officials with each other's systems and, to some extent, to analysts from security agencies in partner countries. Considering that intelligence support to resilience building needs to be done in coordination with other countries as well as other forms of agencies, joint training schemes would be an effective way to establish a solid base for such cooperation.

Second, more interaction between policymakers and intelligence analysts would allow for better appreciation of the roles and needs of each category. Much of the intelligence output from the EU system is today communicated in high level briefings, by senior managers or analysts to

[23] Fägersten, supra note 20.

senior decision makers. Considering the time frame of these decision-makers, briefings are often focused on the most pressing issues of the moment. More interaction and perhaps new forms of interactions further down in the respective hierarchies would lay the ground for intelligence support in different temporal phases, allowing for example the intelligence branch to contribute also to long-term preventive work. Such low-level but continuous interaction would bridge the gaps between the different time horizons with which different parts of the EU bureaucracy work.

Third, more intelligence output within the EU system should be produced as open source, allowing for a more efficient response against hybrid tactics. As discussed above, the aim of hybrid tactics is to increase uncertainty in any given situation. The referent object of such uncertainty could be an official decision-maker but could also just as likely be the general public or more targeted individuals. Therefore, the value of correct information and threat analysis that is fast, open and easily verified is substantial. Considering that multilateral intelligence products rarely are based on the most sensitive information, the step towards making more of the output as open source should be manageable.

Last, also considering that intelligence support might be directed towards partner countries, and that the concept of resilience is rather vaguely defined in EU parlance as discussed above, it is vital that such support live up to the demands set by liberal democratic principles. Intelligence activities are in many political systems tied to oppression and stability of non-democratic regimes. While the Arab spring did not deliver the democratic transitions many hoped for, it did deliver a strong lesson for Western powers aiming to invest in stability in troubled countries of the region. To the extent that European intelligence resources are engaged in the projection of forward resilience, caution will have to guide mission design.