SAIS
JOHNS HOPKINS
SCHOOL of ADVANCED
INTERNATIONAL STUDIES

CENTER FOR TRANSATLANTIC RELATIONS

Forward Resilience: Protecting Society in an Interconnected World Working Paper Series

Temporal Projection of Societal Resilience in the EU: A Dynamic Organisation Approach

Tim Prior[1]

Systemic Societal Resilience, Connectivity and Vulnerability in the EU

Modern Western societies are characterised by global connectedness. Connectedness generally strengthens social systems, yet it can also increase the exposure and sensitivity of social systems to disturbances (natural, technical, and social), because the increasing connectedness of social systems requires increasingly complex system-critical services like transport, communications, energy, finance, or regional security.[2]

The progressive increase in complexity of social-technical systems through time has mirrored a realisation that perfect security is theoretical at best. Despite the evolution and sophistication of risk prevention practices (in both the private and public sectors), threats and hazards cannot be completely avoided, but measures to cope with disturbance can be established. In this context of imperfect societal security, advocating resilience has become a standard cross-scale approach, in many cases tagged on to traditional security policies, rather than being applied as a stand-alone approach.[3]

This brief chapter borrows a theoretical understanding of the nature of vulnerability (considering especially the interplay between sensitivity and exposure to risks and threats) in order to examine the notion of 'forward resilience' in the context of future security challenges in Europe. While Europe's security institutions are built around solidarity, member states are characterised by a set of specific socio-economic, cultural, technical, and political attributes. These attributes influence the countries' abilities to cope with different risks or threats, stressors and disturbances.[4] In this context an understanding of how these attributes translate into important systemic, Union-relevant vulnerabilities is fundamentally important for the resilience of the European Union (EU). As an open system of connected nations, systemically addressing and adapting to vulnerabilities, presents an atypical, but constructive, paradigm for addressing contemporary and future security challenges.

[1] With valuable contributions and suggestions from Aglaya Snetkov, Florian Roth, Andreas Wenger, Christian Nünlist, Oliver Thränert, Linda Maduz, all from the Center for Security Studies at ETH Zurich.

[2] L. K. Comfort, "Risk, security, and disaster management," *Annual Review of Political Science* 8:335-356 (2005);
Susan L. Cutter, "The landscape of disaster resilience indicators in the USA," *Natural Hazards*: 1-18. doi: 10.1007/s11069-015-1993-2 (2005).

[3] F. Roth and T. Prior, "The boundaries of building societal resilience: responsibilization and Swiss Civil defense in the Cold War," *Behemoth. A journal on civilisation* 7 (2):91-111 (2014).

[4] N. Brooks, "Vulnerability, risk and adaptation: A conceptual framework," *Tyndall Centre for Climate Change Research Working Paper*, 38, pp.1-16 (2003).

‘Forward resilience’ is here taken to reflect an approach to project resilience temporally from points of strength, where resources to support resilience exist, to points of vulnerability, in order to increase overall systemic resilience. We draw on several examples of security risks to explore attributions of vulnerability in the European Union. For the purposes of this chapter, we view the EU as systems of connections, where mobility and communication (two key elements influencing locations of exposure and sensitivity in the context of the security risk examined here) connectivity determine center and periphery from a vulnerability perspective, and which are not primarily geographical. In such systems, we suggest that systemic societal resilience, organised by the EU through ad-hoc and distributed foresight, is fundamental in building cross-Union solidarity to security risks, in addressing perceptions of Union vulnerability, and building capacity where necessary.

Vulnerability and Resilience

Very simply, vulnerability is interpreted in a negative sense as the “susceptibility to be harmed.”[5] While in most contexts many factors influence whether someone or something will be harmed, vulnerability is often conceptually composed of three interrelated elements. To be vulnerable something must first be exposed to a risk or threat, and exposure is possibly the most obvious component of vulnerability. Second, to be vulnerable an entity must also be sensitive to the consequences of that risk or threat. Third, vulnerability can be reduced by an entity’s capacity (intrinsic or extrinsic) to adapt to the risk or threat to which it is exposed and sensitive, and is therefore also considered an influential element of vulnerability. Given the component nature of vulnerability, the magnitude of each component’s influence on vulnerability changes with different risks or threats, and in the context of the entity exists.

By contrast, resilience is interpreted in a very positive sense as the ability of a system, person, or entity to withstand, bounce back and cope, and/or adapt to external (or internal) stress or disturbance. This positivity has propelled the popularity of resilience to the forefront of modern transformations in many aspects of security and safety politics (including disaster management, cyber security, critical infrastructure protection, social disturbance, *etc*.).[6] The drive to ‘build’ resilience, to address systemic vulnerability, incapacity, or weakness, is at the heart of these transformations.

Above all, resilience is anticipatory and systemic. Where a traditional security management approach assumes that known risks or threats are manageable through preventive actions, mainly organized and executed through strong centralized structures, adopting a resilience approach acknowledges the existence and persistence of existing risks and the necessity to understand systemic vulnerability in order to prepare for potential future shocks and disturbances. This systemic perspective also requires contributions and responsibility across a broader set of institutions, actors, and civil society, highlighting the necessity of distributed action and reaction responsibilities. From a social systems perspective the notion of resilience draws heavily on the principle of self-organization, which is seen to play a central role as a fundamental precondition for the adaptation of complex, but vulnerable or disturbed systems.

Vulnerability and resilience are closely connected ideas. Indeed, resilient systems can be less vulnerable. However, vulnerability and resilience are also generally considered to be specific to particular risks or threats. This means that something may be vulnerable to one risk, and not to another, likewise one system may be resilient in the context of one risk, but not another. This

[5] W. N. Adger, "Vulnerability," *Global Environmental Change* 16 (3):268-281. doi: 10.1016/j.gloenvcha.2006.02.006, p. 269 (2003).

[6] T. Prior, F. Roth, and M. Herzog, "Transformations in European Natural Hazard Management: There and Back Again," in R. Bossong and H. Hegeman, eds., *European Civil Security Governance: Diversity and Cooperation in Crisis and Disaster Management* (London: Palgrave MacMillan 2003).

specificity of both system characters implies a lack of symmetry between them – as one character rises, the other does not necessarily fall.[7]

A perception of vulnerability can be construed as weakness from a security perspective, but from a resilience perspective, understanding the elements of vulnerability is key to coping with potential disturbances and shocks. The desire to build resilience into systems, especially based on an understanding of the components of vulnerability (risk/hazard, exposure, sensitivity, and adaptive capacity), is closely connected to establishing organisational capacity to quickly respond to risk or threat triggers, and react appropriately.

A Systems View of Center and Periphery

Traditional notions of internal and external security are complicated by the cross-border interdependence of the critical service systems supporting modern societies,[8] especially in the EU and surrounding countries. When countries seek to secure the critical services their populations require, transboundary systems create particular challenges, including in particular sharing management and maintenance responsibilities.

In international politico-economic unions like the EU, dealing with transboundary systemic disruptions should be simplified by existing organisational frameworks. More often though, these unions expose exactly the vulnerability in countries' relationships (witnessed by declining within-union solidarity) that highlight the difficulty of transboundary system management and security. Three risks (or threats, depending on the point of reference) highlight the importance of these issues in the European Union: the current refugee migration crisis, terrorism, and Russia's hybrid 'warfare'. In each of these cases, Union fragility is typically expressed as vulnerability, but not necessarily at the traditional geographic periphery. EU boundary nations such as Greece, Italy, and Austria are inundated by refugees as transit countries, while Germany, Sweden and France face the challenge of settling many of these refuges. Cultural differences expose western European cities to violent extremism and terror attacks in the geographic center of the union. Baltic and Scandinavian country members of the EU are sensitive to 'hybrid warfare', an approach used by Russia in the Ukrainian crisis in 2014, but Germany's reliance on Ukrainian gas for heating also makes it sensitive to similar threats.

These risks challenge the traditional notion of the 'center' and the 'periphery', especially because they are driven by population mobility and cross-Union cultural variability. In the context of these risks or threats it is not clear what is center and what is peripheral. While geographically peripheral Baltic countries might be exposed and sensitive to the threat of hybrid warfare, geographically central countries like France and Germany are exposed and sensitive to risks and threats associated with terrorism and refugee migration. Therefore, projecting vulnerability geographically from a central 'secure' position onto a peripheral 'insecure' position is no longer valid, especially in highly complex, mobile societies like that existing in the EU. Likewise, projecting resilience forward geographically from the center to the periphery also makes little sense given the nature of the modern threat/risk environment. Rather, resilience should be projected forward from positions where threat-specific capacities exist, and where vulnerabilities are lowest.

[7] G. C. Gallopín, "Linkages between vulnerability, resilience, and adaptive capacity," *Global Environmental Change* 16 (3):293-303 (2006).

[8] R. Mugavero, V. Sabato, and C. Stallo, "Territorial Security: Architectures, methodologies and integrated systems for the information management in multi-risk scenarios," *2012 IEEE First AESS European Conference on Satellite Telecommunications (ESTEL)*, 2-5 Oct. 2012.

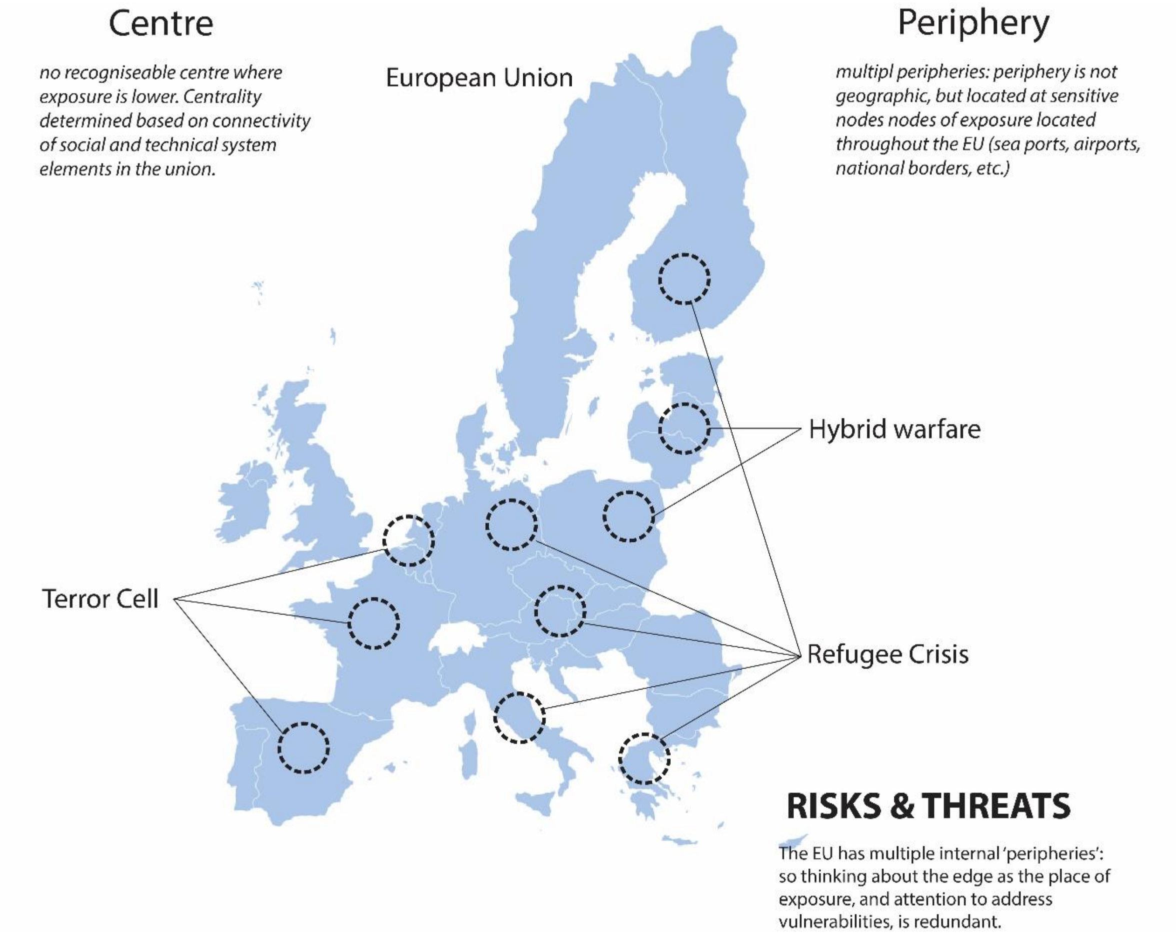
Centre
no recogniseable centre where exposure is lower. Centrality determined based on connectivity of social and technical system elements in the union.
European Union
Periphery
multipl peripheries: periphery is not geographic, but located at sensitive nodes nodes of exposure located throughout the EU (sea ports, airports, national borders, etc.)
Hybrid warfare
Terror Cell
Refugee Crisis
RISKS & THREATS
The EU has multiple internal 'peripheries': so thinking about the edge as the place of exposure, and attention to address vulnerabilities, is redundant.

Figure 1: Multiple peripheries, with no geographic centre in context of risks & threats.

Supporting Societal Resilience Projection with Ad-Hoc Resilience Foresight (Temporal)

While geography has traditionally been a key factor in international politics, increasing connectivity between people, societies, technology, and nations has seen the importance of geography change in international relations. Connectivity and interdependence across domains (social, environmental, economic, political, cultural, technical) implies the need to think of systems rather than of geographies, where systemic connections and linkages across nodes of influence determine the center and periphery of systems. A systemic perspective highlights that the density of nodes of connection reflects influence or importance, where stability develops or dissipates, where resources for resilience exist or don't, where vulnerabilities are reduced or increase. Examining national unions or alliances from a systemic perspective can support cross-Union vulnerability analysis, and the pseudo-temporal projection of resilience using threat foresight and risk scenarios.

Rather than expending resources on strengthening the geographic periphery as a buffer for the center, dedicating the resources to Europe-wide (including external to the Union) foresighting for preparedness will yield a better investment towards regional resilience though a coordinated focus on threats/risks that builds international cohesion and solidarity, close to and beyond a point of focus. There can be no development of societal resilience without establishing a medium to long-term view of vulnerabilities and resilience. In situations of unpredictability or uncertainty, proactive approaches that help decision makers plan for future potential disturbances, and to understand vulnerabilities, can best be used to identify areas of priority for different partners/members, and whether or not a set of common concerns can be discerned. The anticipatory nature of resilience lends itself well to addressing real and perceived cross-Union vulnerabilities. Within the existing organisational structures of the EU, for example, cross-Union resilience requires an investment in foresight practice to anticipate systemically potential risks and threats, which identifies vulnerabilities, and can be drawn on to develop cross-Union adaptive capacities.

Research by Weber, Sailer, and Katzy[9] highlights the way foresight can be used in a fluid and case-specific manner to build resilience, especially within dynamic and unpredictable network circumstances, such those presented by the current unpredictability in threat and risk in the context of the EU. Ad-hoc rather than strategic management-based foresight processes can encourage self-organised decision environments characterised by flexibility and dynamism. In the context of the EU, an 'ad-hoc foresight' approach should then draw on a distributed collaboration among all members and neighbours in a relational manner. While the EU seeks to assure within-Union security through actions of integration and solidarity, establishing a clear picture of the future threat landscape requires the inclusion and cooperation of EU-external neighbour countries. Engaging neighbours in ad-hoc vulnerability foresight would be driven by the results of completed vulnerability foresight practices, which would cue the involvement of additional partners as necessary. The ad-hoc nature of the process is characterised by the ability to engage or disengage partners in response to the changing threat landscape.

Importantly, switching from a centralised approach to strategic foresight to a more self-organised and relational one will require within-Union agreement to engage in an ongoing process to identify, and initially focus on a narrower set of core security priorities. Figure 2 illustrates a prospective conceptualisation of societal resilience based on organisational principles. Effective ad-hoc foresighting to address cross-union vulnerability and build societal resilience would most effectively be undertaken during the 'critical period' as identified by Martin and Sunley,[10] with 'detection' and 'activation' highlighted especially as points at which a distributed ad-hoc foresight and planning process should be undertaken.

A decentralised and ad-hoc approach to foresight for preparedness and resilience also addresses traditional issue myopia (for instance, peripheral vulnerability versus central strength), by devolved and inclusive issue identification and communication. Inclusive processes toward societal resilience through foresight can help to prevent similar issues from recurring. For instance, when security organisation is centralised, without appropriate mechanisms for distributed input in planning, gaining new perspectives on how existing or past

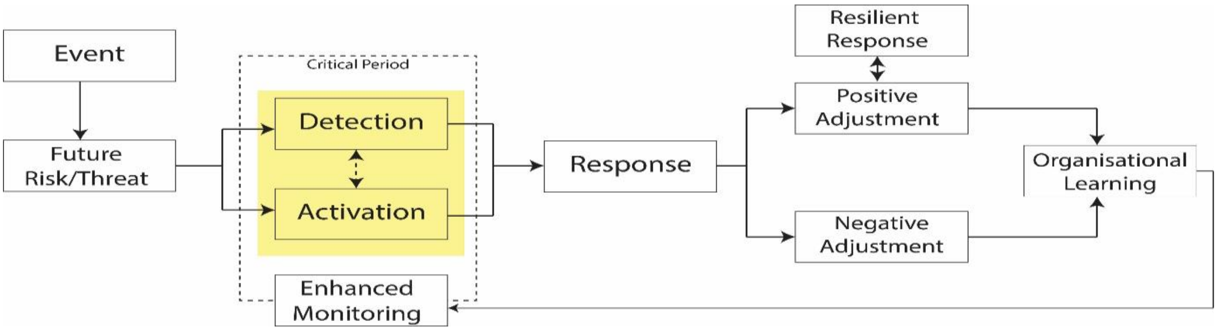

Figure 2: A conception of organisational resilience.[11]

[9] Christina Weber, Klaus Sailer, and Bernhard Katzy, "Real-time foresight — Preparedness for dynamic networks," *Technological Forecasting and Social Change* 101:299-313. doi: http://dx.doi.org/10.1016/j.techfore.2015.05.016 (2015).

[10] Ron Martin and Peter Sunley, "On the notion of regional economic resilience: conceptualization and explanation," *Journal of Economic Geography* 15 (1):1-42. doi: 10.1093/jeg/lbu015 (2015).

[11] Adapted from Ibid.

issues can be solved is limited. Collaborative and distributed ad-hoc foresight could be the basis of an inclusive concept to bring groups/states together across different spaces (systemic and geographic) rather than creating or widening dividing lines, or fomenting competition.

In the EU context, just as collaborative and distributed approaches to vulnerability through foresight for resilience building can increase Union solidarity, so too can solidarity within the EU build resilience. Providing opportunities for, and leveraging the value of local and regional connections beyond the EU, though, is hugely important for building self-organised resilience, and for promoting integrated approaches to addressing vulnerability, encouraging cohesion around key issues among union members, and assuring EU security in the medium to long-term. The capacity of local actors, institutions and organisations to collect context specific threat and vulnerability information can increase trust in local services and build system solidarity. For instance, Baltic countries are sensitive to hybrid warfare, and it is in the national responsibility to ensure security against such threat. Yet, the EU as an integrated collective that wants to ensure critical services to the EU society can support these countries by adopting supportive mechanisms or regulations (like for instance, the Civil Protection Mechanism). The EU must facilitate and coordinate the systemic cohesion of member states around issues of common interest (including risks and threats), rather than permitting regional disintegration. This entails member states recognising and acknowledging that threats across the union differ, and each country's ability to address a particular threat also differs – there are nationally specific social, cultural, political or economic reasons that create a specific country context influencing their actions relating to threats. If members are interested only in addressing issues nationally, then the value of the Union in countering the risks these threats bring is diminished. Additionally, because threats can also originate from outside the Union, with impacts on the union, union members must also recognise and acknowledge that incorporating non-members of the union in threat identification and assessment is also necessary. Non-members are no longer peripheral, but then become central players in identification, assessment and management.

Keys Points, Directions and Recommendations

a) <u>Resilience is anticipatory</u>

The value of the resilience paradigm is its anticipatory nature: uncertainty is accepted, and acceptance is the first step in addressing uncertainty. In this context, forward resilience requires functional anticipation. Foresight is a practical tool for early detection. Forward resilience should be driven temporally through self-organised foresight exercises focussed on threat identification, threat-specific vulnerability assessments, and threat-specific capability assessments. In the same way the EU Civil Protection Mechanism standardises and identifies disaster response resources across the union, results of threat-specific capability assessments should be shared in order to identify resources for addressing threats or mitigating risk, and resource gaps where resources should be directed. Functional anticipation through foresight should precede and determine subsequent physical actions of support or intervention in and outside of the union.

b) <u>Ad-hoc organisation</u>

Functional anticipation in an uncertain threat landscape requires flexible and adaptive participation by multiple actors. Participation in early detection activities should be organised in an ad-hoc manner as required based on threat appearance, not necessarily led by the politically strong or the geographically central. The need for flexibility means avoiding institutionalisation of the anticipatory activities, rather relying on existing, or fostering new operational networks within and between relevant agencies. Even so, these ad-hoc processes must be recognised nationally, and this might effectively be done through institutionally facilitated joint activities (like threat response and risk mitigation exercises) conducted between EU members and near neighbours. Self-organisation differs from facilitated organisation, but aligns with systems resilience thinking.

c) Organisational information sharing and access for proactive planning
Non-institutionalised inter-agency anticipation (foresight) activities must be supported by the creation of a threat/capability information repository to support organisational learning. A multi-national information centre where participants can communicate experiences and identify key lessons can help EU members and neighbours to better understand the type and impact of actual and potential threats. Better ways of sharing information, supported by structures like Europol's Secure Information Exchange Network Application (SIENA), should be the basis for early detection, early warning, and information on capabilities. Europol's European Counter Terrorism Centre also provides an interesting model on which a broader threat information centre might be based, providing operational and strategic support in assessing and responding to threats. Non-EU members must be encouraged to contribute knowledge to this resource.

d) Systemic cohesion for unity
Stability and cohesion in uncertain threat contexts requires unity. In processes of threat anticipation and risk mitigation, unity means finding inclusive mechanisms rather than exclusive ones. This has two implications: first, EU members must acknowledge that threats are perceived and felt differently among the members of the union; second, non-EU countries, whose borders, infrastructures, or other services are shared, also have an important role in threat and risk mitigation. Therefore, information-sharing structures, non-institutional self-organised networks, and anticipatory activities must necessarily involve all actors and should inform a regional threat prioritisation process, which should direct threat mitigation (and ultimately, response) resources to those issues of greatest regional (not national) priority.