UNIO - *EU Law Journal*. Vol. 4, No. 2, Julho 2018, pp 42-47.

"Security Union" and the digital sphere: unpacking securitization processes

Sandra Fernandes*

ABSTRACT: Since 2016, the EU is boosting its agenda on security in a geopolitical context that comprises multiple challenges, namely the fight against terrorism, the migration pressure, relations with Russia, Brexit, and the redefinition of the Euro-Atlantic partnership. This article exposes drivers of the EU's perspective on security, in particular, in the context of the "Security Union" framework and the emergence of the digital sphere as a defence matter.

KEYWORDS: Security Union – securitization – security nexuses – digital – cyber dimension.

* Professor at the University of Minho in the Department of International Relations and Public Administration (School of Economics and Management). Member of the Research Centre of Political Science (CICP).

I. Introduction

The European Union (EU) has been evolving as a security actor with significant transformations since the Lisbon Treaty 2009. In defence matters, we are witnessing a "*brave new world*" for the Union in the sense that there has been noticeable acceleration in the last two years and results are expected from 2018 onwards.

We argue that the promotion of the "Security Union" commissioner under Juncker's leadership promotes an agenda for security that operationalizes security nexuses that define the Union's external action. Additionally, the broadening of the security agenda in terms of internal and external threats blurs the lines between institutions dealing with justice and home affairs and external affairs. This raises the issue of consistency of the Union's policies.

This article aims to give, firstly, an overview of the Union's understanding of security by presenting security nexuses at play and securitization processes. Secondly, the analysis unpacks how the "Security Union" developments reflect this understanding and further presents key developments in the defence realm that tackle the digital/cybernetic dimension of threats.

II. Balancing values and interests: the meaning of "security" for the EU

The EU, as a security actor, has been prominently analysed under two prisms: the security nexuses and the processes of securitisation. These two conceptual frameworks are informative of the Union's vision about what security means and what is constitutive of threats. This section unpacks the main contributions of the two approaches in understanding the rationales that drive the "Security Union" agenda and EU's external action at large.

The EU's political values shape an approach, through which the EU promotes transformation in third countries, namely in its enlargement policy and neighbourhood policy. EU values include respect for human dignity and human rights, freedom, democracy, equality and the rule of law. In the context of enlargement and relations with neighbouring countries, including Russia, the values and principles are defined as follows: the rule of law; good governance; respect for human rights, including the rights of minorities; promoting good neighbourly relations; principles of market economy and sustainable development.[1]

However, the Union also has strategic interests as protracted by Member States and institutions, that also shape its external policies. The postulate is that Brussels prioritizes a normative approach when it emphasizes the rule of law, democracy, and human rights. When framing its decisions in terms of security, it adopts a strategic approach. This dichotomy represents the values-security nexus and produces tensions among EU actors in the promotion of external policies.

The second security nexus is known as "*internal-external*" and results from processes of securitization. The relationship between "inside" and "outside" has long been regarded as central in the EU's security policy.[2] Securitization is a discursive

[1] European Commission, "Communication from the Commission to the Council and the European Parliament on relations with Russia", Brussels, 9 February, COM(2004) 106.

[2] Didier Bigo, "Internal and External Security(ies): The Möbius Ribbon", in *Identities, Borders, Orders: Rethinking International Relations Theory*, ed. M. Albert, D. Jacobson and Y. Lapid. (Minneapolis, University of Minnesota Press, 2006), 91-116; Didier Bigo, "When Two become One: Internal and

process through which a securitising agent is successful in portraying an issue as an existential threat to a referent object and in demanding exceptional measures to tackle that threat. *"Securitisation theory is premised on a constructivist notion of security, in the sense that 'security is a quality actors inject into issues by securitising them"*.[3]

Bigo[4] has developed the analysis on the internal-external nexus, namely concerning the issue of migration. This literature is part of a global approach of the EU security *"actorness"*[5] that is accompanied, in parallel, by the Union's own narrative on the nexus: internal-external, security-development, civilian-military, public-private.[6] The thinking about the security nexus is, thus, also driven by the *"securitization"* concept that highlights the role of the externalisation of internal security for the legitimation of the EU's role.[7]

Additionally, the merging of internal and external security has prompted the creation of an external dimension of the EU area of Justice and Home Affairs that seeks to promote the rule of law in neighbouring countries. Each specific policy field needs to be analysed in order to understand how the EU displays simultaneously normative and strategic intents, as opposed to assuming a strict dichotomy to define its actions.[8]

The literature concerning the EU as a normative/security power is, thus, related to the thinking about the internal-external security nexus. As Traunert underlines, the comprehensive coherence of EU foreign policy is at stake depending on the balance between values and priorities. *"One of the major challenges for the EU has been to ensure that the mainstreaming of internal security objectives in the EU's external relations does not undermine the normative aspirations of EU foreign policy-making*".[9] He underlines the relegation of values in favour of security concerns, specifically in the area of Justice and Home Affairs.

III. "Security Union" and the digital/cybernetic dimension of security

We argue here that the "Security Union" policy area is framed under the two above-mentioned nexuses and processes of securitization. This understanding originates the agenda for security of the EU and the means that it ought to develop. One of the main objectives of the European Commission is to *"address the existing shortcomings of EU information systems for security and border management*." Additionally, it incorporated the aim "*to counter radicalisation and the cyber threat."*[10]

External Securitisations in Europe", in *International Relations Theory and the Politics of European Integration, Power, Security and Community*, ed. M. Kelstrup and M. C. Williams. (London: Routledge, 2001), 320-360.

[3] Barry Buzan, et al, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner Publishers, 1998): 204.

[4] Didier Bigo, *Internal and External…*

[5] Charlotte Bretherton and John Vogler, *The European Union as a Global Actor* (London: Routledge, 2006).

[6] Ana Paula Brandão, "The Internal-External nexus in the security narrative of the European Union", *JANUS.NET e-journal of International Relations* 6(1) (2015).

[7] Didier Bigo, *Internal and External…*; Barry Buzan *et al.*, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner Publishers, 1998).

[8] Nicole Wichmann, "Promoting the rule of law in the European neighbourhood policy: Strategic or normative power?", P*olitique européenne* 22(2) (2007): 81-104.

[9] Florian Traunert, "The internal-external security nexus: more coherence under Lisbon?", *EUISS Occasional Paper*, 89 (2011): 21.

[10] European Commission, "Commission delivers on interoperability and measures to fight terrorism

The idea that security under the Justice and Home Affairs portfolio has to be integrated in a comprehensive approach is, thus, materialized in the "Security Union" that merges internal and external threats. As far as the emergence of the digital dimension is concerned, a process of securitization has brought home the idea that we are more vulnerable because there is no security setting for how we relate to the world.[11]

The EU's view is about creating a European agenda for security where information systems need to be defended and resilient. This agenda is fast evolving and widening. For instance, in the prism of "external border", the dimension of combating hybrid threats was introduced in April 2016 with a "*Joint Framework*".[12] The Union is progressing towards a definition of these threats that comprises *"non-conventional forms, such as radicalisation leading to terrorist attacks, chemical attacks, cyber-attacks or disinformation campaigns*." They *"combine conventional and unconventional, military and non-military activities that can be used in a coordinated manner by state or non-state actors to achieve specific political objectives"* that resume to endanger European societies and EU values.[13]

Beyond emerging agendas and technical issues, such as the creation of interoperability of EU information systems for borders and security[14], there is a geopolitical context that explains why the Union is producing this specific set of policies to address external threats. The geopolitical situation in its immediate vicinity has turned the fight against terrorism into a priority and the migration pressure a security issue, resulting from a process of securitisation. Additionally, the degradation of relations with Russia in the aftermath of the annexation of Crimea in March 2014 has highlighted the digital/cybernetic threats in the context of methods of hybrid warfare.[15]

The creation of the East Stratcom Task Force, in 2015, at the European External Action Service exemplifies the above-mentioned understanding. The Task Force received funding from the EU budget for the first time, for the 2018-2020 period.[16] The body aims to raise awareness and understanding of disinformation and improve the Union's own performance concerning its news and communication and support to journalism in Eastern Europe.

Taking into account the nexus between internal and external threats and the balance between security and the normative concerns, above-mentioned, EU policies

---

and the cyber threat" (2017).

[11] James Morrison, Address at the Annual Policy Security Summit "Europe's tough neighbourhood: urgent challenges in a complex environment", Friends of Europe, Brussels, 28 November (2017).

[12] European Commission, "An European Agenda on Security. State of Play", June (2017).

[13] European Union External Action Service, "A Europe that Protects: Countering Hybrid Threats", 13 June (2018), https://eeas.europa.eu/headquarters/headquarters-homepage/46393/europe-protects-countering-hybrid-threats_en.

[14] European Parliament, "Interoperability between EU information systems (police and judicial cooperation, asylum and migration)", Procedure File 2017/0352(COD), 2018.

[15] LeBrun defines hybrid warfare as follow: "*the concept is currently used to describe and denounce Russian actions in Ukraine and influence operations in the informational sphere as well as cybernetic and covert actions. (...) Remnant Soviet-style tactics of manipulation, deception, and disinformation are crucial in achieving military success without engaging military forces, as it would favor the internal decay of target societies and sow defeatism and induce compliance. (...) Whatever the preferred terminology, Russia builds and thinks its coercion instruments along to full-spectrum posture. Technological and informational capacities are enablers of all other dimensions of conflict*". See Maxime LeBrun, "Sitting on the Fence: The 'Hybrid' Moment", ICDS, 11 October, (2017).

[16] Jennifer Ranking, "EU anti-propaganda unit gets €1m a year to counter Russian fake news", The Guardian, November 25, 2017.

to address security needs can be found in several dimensions of the European process of integration. The broader framework of the "comprehensive approach" sustains this understanding. This approach was formulated in 2016 and is further complemented by the EU Global Strategy of the same year.[17] The bottom line is the will to use the Union's tools in a more coherent way, including an inter-institutional perspective.

In this broader context, an emphasis on defence is taking place with, for instance, advancements in the military sphere such as Permanent Structured Cooperation (PESCO) and a tightening of EU-NATO cooperation. PESCO results from the provisions of the Lisbon Treaty and was adopted by 25 Member States in December 2017. Among the 17 projects that are being developed, several include the cyber domain.[18]

The cooperation with NATO highlights the cyber dimension as well and EU-NATO joint work is instrumental in the EU's view. Since December 2016, initiatives include the participation of the Union in NATO's cyber exercises, the exchange of military concepts, interoperability and staff-to-staff contacts.[19]

In the words of the Head of Cabinet to European Commissioner for Security Union, both the end of the peace dividend and of the financial crisis explain today developments such as PESCO, as compared to the post-Treaty of Lisbon period.[20] Additionally, the cyber threat is so massive that it demands collective action and responsibility. The costs of developing tools in the cyber domain are high and PESCO can be a facilitator because it demonstrates the linkage of digital to the field of defence that is increasingly complex, comprehensive, and integrated.

IV. Conclusion

The EU is confronted with many security challenges that require multiple forms of defence and resilience. The steps towards digital interoperability in several domains such as Justice and Home Affairs or tackling cyber threats are part of processes of securitization that comprise two elements. On the one hand, the Union is increasingly viewing threats as being internal and external in nature. Consequently, on the other hand, the policies and instruments to address these threats have to engage all the portfolios of EU actors.

The first accelerator of the incorporation of the digital dimension in the EU's security policies is, thus, the European Commission's new ambition to bring security and defence to the core of the EU. The second factor is the new external environment that includes challenges such as migration, Russia, the distancing by the United States, a traditional ally with growing isolationist proclivities, and Brexit.

---

[17] High Representative of the European Union for Foreign Affairs and Security Policy. Joint communication to the European Parliament and the Council, The EU's comprehensive approach to external conflict and crises. Brussels, 11.12.2013 JOIN(2013) 30 final (2016).

[18] Council of the European Union, "Defence cooperation: Council adopts an implementation roadmap for the Permanent Structured Cooperation (PESCO)", (2018), http://www.consilium.europa.eu/en/press/press-releases/2018/03/06/defence-cooperation-council-adopts-an-implementation-roadmap-for-the-permanent-structured-cooperation-pesco/.

[19] NATO, "Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization", (2016) https://www.nato.int/cps/ua/natohq/official_texts_138829.htm.

[20] James Morrison, *Address…*

As underlined by Morrison[21], the cyber domain is a team sport more than any other domain. The growing cooperation with NATO in this field since 2016 is one of the signals of this understanding. However, investment in defence is based on risks and the notion of risk in the cyber area is not yet direct for all Member States with significant differences among them. The Baltic States, and particularly Estonia, have been very active in promoting the digital and cyber dimensions of EU (and NATO) security.[22] The way forward for the Union in this domain is, arguably, a process of securitization that will shape new policies and tools, beyond the ongoing agenda on interoperability.

[21] James Morrison, *Address*…

[22] Sandra Fernandes and Daniel Correia, "(Re)Securitization in Europe: the Baltic States and Russia", *Debater Europa* 18 (2018): 103-129.