SECURITY & STRATEGY No 131
October 2017

Royal Higher Institute for Defence

DEFENCE

Countering "Hybrid Threats": Belgium and the Euro-Atlantic Strategy

Estelle Hoorickx

October 2017

Countering "Hybrid Threats": Belgium and the Euro-Atlantic Strategy

Estelle Hoorickx

Translated from French by Alban Bourguignon
Department Productions, Public Relations and Support

Royal Higher Institute for Defence
Centre for Security and Defence Studies
30 avenue de la Renaissance
1000 Brussels

ISSN 2295-0915

Any question, commentary or remark related to this document can be addressed to:
Director of the Centre for Security and Defence Studies
Royal Higher Institute for Defence
30 avenue de la Renaissance
1000 Brussels
or by e-mail to: irsd-cesd-scvd@mil.be

The Author

Air force Captain-commandant Estelle Hoorickx is a research fellow at the Centre for Security and Defence Studies in the Royal Higher Institute for Defence (RHID). Her areas of expertise include the conceptual developments in the use of defence capabilities, terrorism in Europe and Belgium's role in international organisations. She is currently completing a PhD in History on Belgium's influence within NATO during the Cold War.

Executive Summary

The practices of "hybrid warfare" are seen as a major security challenge by the EU and NATO, which have been working both separately and cooperatively since 2015 to develop a coherent strategy in the fight against "hybrid campaigns" with the purpose of helping Member States counter this complex threat. The notions of "hybrid threats", or "hybrid warfare" as favoured by NATO, are not unanimously supported nor univocally understood by either organisation nor, for that matter, within either institution. Even though Belgium has not developed a centralised approach to "hybrid threats" to this day, it has addressed the problem through the bias of several bodies responsible for coordinating the country's security policy, no matter the estimated threat level, whether "hybrid" or not. In his latest *Strategic Vision for Defence* issued in June 2016, the Belgian Defence Minister has himself acknowledged the importance of "hybrid warfare".

This study is in two parts. The first part will consider the origins and development of the "hybrid warfare" concept, particularly within the EU and NATO. The second part will explore the various strategies implemented by both organisations as well as Belgium's involvement in the fight against hybrid threats.

Table of Contents

List of Abbreviations and Acronyms

ACOS Ops & Trg	Staff Department for Operations and Training
CBRN	Chemical, Biological, Radiological and Nuclear
CERT	Computer Emergency Response Team
CFSP	Common Foreign and Security Policy
CGCCR	Governmental Crisis and Coordination Centre
CH CRISP	Courrier hebdomadaire du Centre de recherche et d'information socio-politiques (CRISP) (Weekly review of the Centre for Socio-Political Research and Information)
CSDP	Common Security and Defence Policy
CUTA	Coordination Unit for Threat Assessment
DIMEFIL	Diplomatic, Information, Military, Economic, Financial, Intelligence and Law Enforcement
EEAS	European External Action Service
EU	European Union
(EU) INTCEN	(European Union) Intelligence and Situation Centre
EUMS	European Union Military Staff
FoP	Friends of the Presidency Group
GDP	Gross Domestic Product
IISS	International Institute for Strategic Studies
IS	Islamic State
ISIL	Islamic State of Iraq and the Levant
MoD	Ministry of Defence
NATO	North Atlantic Treaty Organisation
NIS	Network and Information Security
NMSG	NATO Modelling and Simulation Group
NSA	National Security Agency
PACE	Parallel and Coordinated Exercise
PD	Parliamentary document
PSC	Political and Security Committee
RAP	Readiness Action Plan
RDN	Revue Défense Nationale
RFAF	Russian Federation Armed Forces
RHID	Royal Higher Institute for Defence
RMA	Royal Military Academy
SIPRI	Stockholm International Peace Research Institute
StratCom	Strategic Communications
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
USSR	Union of Soviet Socialist Republics
VJTF	Very High Readiness Joint Task Force

Introduction

"Hybrid threat? Did you say hybrid threat?" Indeed, it is tempting to use the famous French movie quote for an expression that is nowadays going viral. Georges-Henri Soutou explains the current success of this concept with the very evolution of an international system that is both complex and "blurred", giving rise to strategies that can only be, in a manner of speaking, hybrid, and that answer to threats linked to a certain dematerialisation of conflicts[1]. According to J-.Ch. Coste, "[t]his blur offers to some states, in today's international system which is overall frozen by the balance of the nuclear deterrence, the opportunity to resort to a new form of conflictuality, in which private belligerents can also intervene"[2].

The present study aims to deal with the "hybrid threats" or "hybrid warfare" practices, which the EU and NATO have been considering for some years as a major security challenge. The objective will be to figure out the semantic complexity of this terminology, but also to understand the new geopolitical issues related to it. Belgium's involvement within the EU and NATO in order to address these issues is a major underlying theme of this study.

Although "hybrid warfare" is central to many works, few of them systematically examine the EU and NATO involvement in this matter. The present analysis is based on these two organisations' official positions.

This study consists in two parts and a conclusion. The first part aims to consider the origins and development of the "hybrid warfare" concept, particularly within the EU and NATO. In this framework, we will see, through a meticulous historical approach, that this semantic construction is far from winning unanimous support. The second part explores the various strategies implemented by both organisations in countering hybrid threats as well as the actions taken by Belgium to contribute to these strategies. In conclusion, a number of reflexions focus on the opportunity to resort to the buzz word "hybrid warfare", with a view to redefining the contemporary defence strategies and considering an appropriate involvement in today's geopolitical issues.

[1] G.-H. Soutou, Éditorial, in *Stratégique*, No 111, Paris, 2016, p. 8; G.-H. Soutou, "La stratégie du flou", in *Politique Magazine*, No 131, July-August 2014.

[2] J-C. Coste, "De la guerre hybride à l'hybridité cyberélectronique", in *Revue Défense Nationale (RDN)*, March 2016, p. 23.

Part 1: "Hybrid threats": definitions and issues

The first part of the present study aims to consider the origins and development of the "hybrid warfare" concept, particularly within the EU and NATO. In this framework, we observe to what extent this relatively new semantic construction causes confusion and why it is far from winning unanimous support.

"Hybrid warfare": semantic and geographical reality

In reference dictionaries, the word "hybrid" is associated with categories as diverse as biology, agriculture or linguistics. In English language dictionaries, the adjective always refers to something which is "[d]erived from heterogeneous or incongruous sources; having a mixed character; composed of two diverse elements"[3]. In colloquial French, however, the word "hybrid" can also refer to something "unclearly defined, vague"[4]. It is not before the early 2000s that the adjective "hybrid" is used for the first time in association with an armed conflict.

Two strands of thinking attempted at that time to define the concept of "hybrid warfare". On the one hand, the "kinetic kit" school, which only considers the kinetic aspect of hybrid warfare, describes it as the combination of regular[5] and irregular[6] military forces and tactics. William J. Nemeth is the first supporter of this school of thought to use, in 2002, the expression "hybrid warfare" to define the "Chechen insurgency", which he describes as a "model for hybrid warfare"[7] and "the contemporary form of guerrilla warfare"[8] as this "asymmetric" warfare[9] is a "continuation of pre-state warfare that has become more effective because it employs both modern technology and modern mobilization

[3] *Oxford English Dictionary online* (http://www.oed.com/view/Entry/89809?redirectedFrom=hybrid#eid).

[4] "*D'une nature mal définie, vague*". *Nouveau Larousse Universel*, 1948, p. 955.

[5] Regular warfare is characterised by the use of capital-intensive equipment, an army that represents a state, controls a territory and a population, and defends a front line (E. Tenenbaum, "Guerre hybride: concept stratégique ou confusion sémantique ?", in *RDN*, March 2016, p. 33).

[6] According to H. Coutau-Bégarie, warfare is "irregular" when it is "waged by combatants without status and not pertaining to a regular army, i.e. an army which is established and maintained by a sovereign power" (H. Coutau-Bégarie, "Guerres irrégulières : de quoi parle-t-on ?", in *Stratégique*, January 2009, No 93-96, p. 15). In irregular wars, resorting to guerrilla warfare, ambushes but also terrorism and propaganda are common practice (E. Tenenbaum, *op. cit.*).

[7] William J. Nemeth, *Future War and Chechnya: a Case for Hybrid Warfare*, thesis, Monterey, 2002, p. V.

[8] *Ibid.*, p. 29. "Guerrilla warfare" is defined as "military and paramilitary operations conducted in enemy held or hostile territory by irregular, predominantly indigenous forces" (*NATO glossary of terms and definitions (English and French)*, AAP-6 (2010), p. 2-G-4).

[9] For Colonel Philippe Boone, "[a]symmetrical warfare is the absence of symmetry between the goals, objectives and means of warring forces". In other words, it is about a "conflict opposing combatants whose forces cannot be compared; where the military, sociological and political disproportion between warring sides is total. A conflict where a strong regular army fights against an a priori weak guerrilla movement [or] a nation against a terrorist movement" (A. Martin and L. Coriou, "Définir un conflit asymétrique", in *Le Monde*, 31 March 2003, https://www.lemonde.fr/international/article/2003/03/31/definir-un-conflit-asymetrique_315022_3210.html).

methods"[10], and operates "outside the conventions"[11]. Coming from the same school of thought, Max Boot considers the recent Russian intervention in Crimea as an example of "hybrid warfare" where "heavy armour" and "special forces" have been deployed (the so-called "little green men"[12])[13].

On the other hand, the so-called "full spectrum" school or, according to NATO terminology, the "DIMEFIL spectrum" school[14], which has more supporters than the first movement, includes in its definition of hybrid warfare not only kinetic manoeuvres, i.e. what is referred to as "hard power" (coercion or "hard way"), but also non-kinetic actions, or "soft power"[15], which hybrid warfare uses in order to achieve specific objectives[16]. The nature of those objectives makes it possible to distinguish "hybrid warfare" from "hybrid conflict". Indeed, contrary to hybrid warfare, the goal of "hybrid conflict" is not to injure, diminish or destroy the enemy, but only to influence its behaviour so that he complies with its adversary's will[17]. In a "hybrid conflict", belligerents do not use armed forces, but military intimidation and economic, political, diplomatic or technological pressure tools[18]. Moreover, the enemy's following several methods used during hybrid wars and conflicts is a "hybrid threat", consequently considered as being "multidimensional"[19].

US General James Mattis and US Colonel Frank Hoffman, supporters of the "full spectrum" school of thought, intended to draw the first lessons from the chaos that seized Iraq[20] and defined hybrid warfare in an article released in 2005 in *U.S. Naval Institute Proceedings*[21]. E. Tenenbaum resumes their words by stating that the situation in Iraq after the US intervention is characterised at

---

[10] William J. Nemeth, *Future War and Chechnya: a Case for Hybrid Warfare*, thesis, Monterey, 2002, p. 29.

[11] *Ibid.*, p. 70. In conventional wars, regular armies equipped with high-technology weapons are contending with other regular armies equipped with high-technology weapons. Unconventional wars are characterised by guerrillas waged by irregular armed groups using light weapons with a very low technological level (L. Henninger, "La 'guerre hybride' : escroquerie intellectuelle ou réinvention de la roue ?", in *RDN*, March 2016, p. 51).

[12] The "little green men" – Russian Special Forces without insignia observed in Crimea – could not be correctly identified nor could their presence be properly called an aggression. The aim was to manoeuvre while resorting to an interpretation of the international law (J. Henrotin, "La guerre hybride comme avertissement stratégique", in *Stratégique*, No 111, Paris, 2016, pp. 19-20; E. Tenenbaum, "La manœuvre hybride dans l'art opératif", in *Stratégique*, No 111, Paris, 2016, p. 52).

[13] European Defence Agency, *Hybrid Warfare Threats – Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 November 2015 [SCS/P003198], p. 12.

[14] The acronym "DIMEFIL" stands for "diplomatic, information, military, economic, financial, intelligence and legal".

[15] J. Clech defines "soft power" as the trade and financial coercive measures relating for instance to culture, mass media, social networks or propaganda (J. Clech, "L'hybridité : nouvelles menaces, inflexion stratégique ?", in *RDN*, March 2016, pp. 12-13).

[16] European Defence Agency, *Hybrid Warfare Threats – Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 November 2015 [SCS/P003198], p. 9.

[17] I. Mayr-Knoch, N. Mair and J. Mittelstaedt, "Plaidoyer pour une stratégie hybride de l'Union européenne", in *RDN*, March 2016, p. 45.

[18] P. Pawlak, *At a glance. Understanding Hybrid Threats, European Parliamentary Research Service*, https://epthinktank.eu/2015/06/24/understanding-hybrid-threats/, 24 June 2015.

[19] *Ibid.*

[20] E. Tenenbaum, "La manœuvre hybride dans l'art opératif", in *Stratégique*, No 111, Paris, 2016, pp. 43-44.

[21] J. N. Mattis and F. Hoffman, "Future Warfare: the Rise of Hybrid Wars", in *U.S. Naval Institute Proceedings*, November 2005, Vol. 131, No 11, pp. 18-19.

that time by "a 'post conflict' state of violence resulting from the security vacuum caused by the Ba'ath regime's downfall, an intercommunity and interfaith civil war, an insurgency against the foreign occupation, international terrorist activities, as well as a potential risk of disseminating weapons of mass destruction"[22]. The term was later reused during the war waged by Israel against Hezbollah in Lebanon in 2006. Israel appeared to be in a difficult situation facing an adversary which, although irregular and asymmetric, showed itself to be able to manoeuvre tactically and to oppose to Israel's firepower the use of technical means, such as guided missiles or drones, which had only been used by regular national armies up to then[23].

More recently, the notion of "hybridity" resurfaced on the occasion of the armed or unarmed Russian interventions in Estonia (2007)[24], Georgia (2008)[25] and, finally, Ukraine (2014)[26]. During the Russia-Ukraine crisis, the Russian posture is characterised, according to some authors, by the use of a "threshold war" making it possible to generate strategic effects without being subjected to the consequences of a military operation in due form[27]. Such conducts can deeply destabilise the international community, which appears to be unable to respond, in particular with military means[28]. Hybrid warfare includes here a number of practices falling under Russia's overall strategy, which is characterised by the use of one or several ambiguous factors, such as the possibility to achieve an invasion with "little green men" without suffering military consequences in return, Russia's use of "proxies", i.e. forces acting by proxy in favour of third parties and militarily supported by them[29], the

[22] E. Tenenbaum, "Guerre hybride: concept stratégique ou confusion sémantique ?", in *RDN*, March 2016, p. 32.

[23] *Ibid.*

[24] In April 2007, Estonia was victim of a series of unprecedented cyberattacks against its official sites, banks and media, after a Soviet-time war memorial was removed from a park in Tallinn (T. Selhorst, "Russia's Perception Warfare. The Development of Gerasimov's Doctrine in Estonia and Georgia and its Application in Ukraine", in *Militaire Spectator*, No 4, 2016, pp. 154-155).

[25] In August 2008, Georgia launched a military offensive against its separatist province South Ossetia, where the pro-independent feelings had been poisoning Georgia's political life for fifteen years. In response to this, Russia sent tanks and artillery in order to protect the population of this region, which for the most part possesses a Russian passport. About ten days after the hostilities began, a ceasefire was finally signed. During that war, Russians made extensive use of propaganda ("information warfare") and carried out cyberattacks against the main Georgian servers (T. Selhorst, *op. cit.*, pp. 155-157).

[26] J-C. Coste, "De la guerre hybride à l'hybridité cyberélectronique", in *RDN*, March 2016, p. 19. The crisis in Ukraine is an international diplomatic crisis subsequent to the occupation of the Crimean peninsula by unidentified pro-Russia troops, then to Russian troop movements near the border with Ukraine as of 27 February 2014, following the pro-European demonstration called "Euromaidan", that resulted in the fall of pro-Russian Ukrainian President Viktor Yanukovych. On 18 March 2014, following a referendum, the Russian government announced that the Republic of Crimea and the City of Sevastopol became two new federal subjects of the Russian Federation. The international community protested against this political development. The Crimea crisis is followed in early April 2014 by the war in Donbass, in the south-east of Ukraine, where a separatist armed insurgency is still opposing Kiev's central government. Russia is accused of providing military support to the insurgents (A. Dumoulin, "Crise russo-ukrainienne. Conséquences sur les politiques de défense de l'OTAN, UE et de défense nationale", in *Sécurité & Stratégie* (RHID), No 125, June 2016, pp. 3, 6-8 and 15).

[27] J. Henrotin, "La guerre hybride comme avertissement stratégique", in *Stratégique*, No 111, Paris, 2016, p. 20.

[28] *Letter of the Defence Policy Directors of 10 Northem Group Nations to EEAS DSG*, Maciej Popowski, 17 February 2015.

[29] The use of "*proxies*", particularly during the operations in Donbass, enabled to circumvent international law in order to undermine the legal base for a juridically legitimate response (E. Tenenbaum, "La manœuvre hybride dans l'art opératif", in *Stratégique*, No 111, Paris, 2016, p. 20). Ultimately, *proxy* warfare is a "compound warfare" consisting in the simultaneous use of a main force and guerrilla forces against an enemy, leading to the creation of a "hybridation compounding both (concentrated) conventional and unconventional forces as well as (scattered) unconventional forces at the same time" (*Ibid.*, p. 23).

possibility to use exportations as political pressure tools and, more generally, the use of all power resources in order to achieve strategic objectives[30]. Russia's use of digital weapons for subversive goals in Estonia in 2007, in Georgia in 2008 and, more recently, in Crimea is also considered as a hybrid operational mode[31]. In 2009, Frank Hoffman defined hybrid threat as "[a]ny adversary that simultaneously and adaptively employs a fused mix of conventional weapons[32], irregular tactics, terrorism and criminal behavior in the battle space to obtain their political objectives[33]". As we will see in the next chapters, this point of view will find some institutional echo with the EU and NATO.

Some currently consider the organisation Islamic State (IS) as a "hybrid actor" able to achieve real operational successes[34]; indeed, it achieved a major territorial expansion in Syria and Iraq, peaking in 2014[35]. According to E. Tenenbaum, IS carries out a certain type of hybrid manoeuvres which fall under what could be called a "techno-guerrilla"[36]. J. Henrotin affirms that IS constitutes indeed "the most achieved form of hybrid enemy"[37]. It is "the incarnation of the nightmare […]: a fundamentally irregular group […] combining […] the use of terrorism and guerrilla as tactical action modes, with modern technologies. […] The hybrid warfare […] [used by the organisation is] a real military operational strategy including the pursuit of an influence strategy/psychological war strategy, and both a material and human resources strategy, as well as the use of a proto-air strategy, or even improvised chemical and biological weapons"[38]. Stéphane Taillat states that the active presence of IS on the social networks for propaganda purposes also constitutes an important element of the hybrid manoeuvre[39]. According to Hervé Pierre, "although possessing a territory, a population and a form of government, Daesh is (fortunately) not recognised as a 'state' and therefore remains, as it does not fit into the international system, a 'private' organisation, admittedly, though a 'private' organisation excelling in adopting hybrid postures. Terrorist attacks committed abroad […] on 'soft' targets with strong media and psychological impact are combined with actions by conventional-type military units opposing, in Syria as in Iraq, force to force"[40]. [In the case of Daesh,] "the qualification of 'hybrid' therefore

---

[30] *Ibid.*, pp. 19-20.

[31] S. Taillat, "Un mode de guerre hybride dissymétrique ? Le cyberespace", in *Stratégique*, No 111, Paris, 2016, p. 89; A. Dumoulin, "Crise russo-ukrainienne. Conséquences sur les politiques de défense de l'OTAN, UE et de défense nationale", in *Sécurité & Stratégie* (RHID), No 125, June 2016, pp. 6 and 15.

[32] In NATO terminology, a conventional weapon is a "weapon that is neither chemical, biological, radiological nor nuclear" (*NATO glossary of terms and definitions (English and French)*, AAP-6 (2010), p. 2-C-15).

[33] F. Hoffman, "Hybrid vs. Compound War-The Janus Choice: Defining Today's Multifaceted Conflict", in *Armed Forces Journal*, October 2009 (http://armedforcesjournal.com/hybrid-vs-compound-war/).

[34] E. Tenenbaum, "La manœuvre hybride dans l'art opératif", in *Stratégique*, No 111, Paris, 2016, p. 56.

[35] *Ibid.*, pp. 56-57.

[36] E. Tenenbaum, "La manœuvre hybride dans l'art opératif", in *Stratégique*, No 111, Paris, 2016, p. 57. Christian Malis defines techno-guerrilla as a warfare mode combining some classical guerrilla tactics with other, more innovative tactics (*swarming*), and associates with this mode the use of advanced technologies such as drones or antitank missiles (Chr. Malis, "Guerre hybride et stratégies de contournement", in *RDN*, March 2016, p. 27).

[37] J. Henrotin, "L'État islamique, forme la plus aboutie de l'ennemi hybride ?", in *DSI*, special edition No 40, December-January 2015.

[38] *Ibid.*, p. 38.

[39] S. Taillat, "Un mode de guerre hybride dissymétrique ? Le cyberespace", in *Stratégique*, No 111, Paris, 2016, pp. 89 and 95.

[40] H. Pierre, *(Re)penser l'hybridité avec Beaufre*, *Stratégique*, No 111, Paris, 2016, p. 41.

becomes the trademark of fighting groups which are sociologically irregular but possess certain key capabilities considered as advanced, and that seemed previously the trademark of regular strategies"[41].

Moreover, it has to be noted that the use of hybrid methods does not seem to be peculiar to Russia or IS. Indeed, according to the European Defence Agency, "China's activities in the South China Sea show a masterful use of the non-kinetic components of hybrid warfare"[42]. As China aims to occupy a major strategical position in that region, it has been implementing there, since 2014-2015, its "Three Warfares" doctrine, which was adopted in 2003, and "envisages warfare on the psychological, media and legal levels, with the overall purpose aimed at achieving [its] strategic goals without resorting to kinetic warfare"[43]. Beijing accordingly appropriated *de facto* the Sansha municipality (Sansha being the name given by China in 2012 to all emerged lands in the central area of the South China Sea), although this maritime area is claimed by Vietnam and Taiwan and has no legal recognition[44]. However, China has been organising tourist trips in these emerged lands since 2013, which is causing tensions in this region[45]. This plan is completed by the large-scale construction of port and airport facilities on reefs in the central area of South China Sea[46].

There are claims that Iran also uses certain elements of the hybrid warfare spectrum in order to increase its influence in the Middle East. As of May 2003, in the aftermath of Operation Iraqi Freedom, Iran would indeed have infiltrated government agents into the Iraqi refugees who were returning to Iraq. H. Gardner adds that Iran blazed a trail for Moscow in revealing how "little green men could be used [in Ukraine] as effective political-military tools against their respective neighbors"[47]. The Iranian military and financial support of Shiite militias in Iraq and Hezbollah in Lebanon as well as its use of proxy forces in those countries to extend its influence are also considered as a form of hybrid warfare[48]. Hall Gardner associates here hybrid warfare with a new form of "brinksmanship"[49]. The goal would indeed be to take advantage of the social, political, economic and military gaps in the rivals' defences, in this case Israel and the United States, by using different kinds

---

[41] E. Tenenbaum, "La manœuvre hybride dans l'art opératif", in *Stratégique*, No 111, Paris, 2016, p. 46.

[42] European Defence Agency, *Hybrid Warfare Threats – Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 November 2015 [SCS/P003198], p. 41.

[43] *Ibid.*, p. 31.

[44] In July 2016, the Permanent Court of Arbitration in The Hague confirmed the existence of an international area in the middle of the South China Sea, thus invalidating any claim on territorial waters in the area. However, Beijing declared that the decision of the judges was "null and void" [J.-V. Brisset, "Quand Steve Bannon prédit un conflit en mer de Chine du Sud : le conseiller spécial de Donald Trump est-il un lucide ou un dangereux va-t-en guerre ?", in *Atlantico*, 3 February 2017 (www.atlantico.fr); L. Defranoux, "Dix questions pour comprendre le conflit en mer de Chine méridionale", in *Libération*, 12 July 2016 (www.libération.fr)].

[45] F. Lelièvre, "Le tourisme, l'autre arme de Pékin pour conquérir la mer de Chine du Sud", in www.letemps.ch, 26 May 2016.

[46] J.-V. Brisset, *op. cit.*

[47] H. Gardner, "Hybrid Warfare: Iranian and Russian Versions of 'Little Green Men' and Contemporary Conflict", in *Research Paper NATO Defense College*, Rome, No 123, December 2015, p. 6.

[48] United States Army Special Operations Command, *Counter-Unconventional Warfare-White Paper*, 2014, pp. 5 and 8 (https://info.publicintelligence.net/USASOC-CounterUnconventionalWarfare.pdf); C. Macé, "L'Iran, soutien sans faille de Damas", in *Libération*, 13 December 2016 (www.libération.fr).

[49] H. Gardner, *op. cit.*, p. 4.

of attacks or threats in succession or simultaneously, with the ultimate purpose of undermining their hegemony in the region[50].

Although the concept of hybrid warfare comprises a vast geographical and semantic reality, it remains largely associated with the methods used by Russia in Ukraine[51]. The next section aims to demonstrate that some even consider Russia's hybrid strategy as the "dark side of the comprehensive approach".

Russia's hybrid strategy: the dark side of comprehensive approach?

According to the European Defence Agency, EU Member States are "particularly vulnerable to non-kinetic variants of hybrid warfare because their societies and institutions are decentralized and democratic"[52]. Autocracies have indeed more direct control over numerous civilian power instruments, such as the economy and the media, in comparison to democratic states, and even more to the European Union[53]. "Furthermore", according to I. Mayr-Knoch, "laws and morally accepted behavior prohibits the use of many clandestine instruments for democracies. This is not the kind of problem autocracies have to cope with"[54]. Against this background, it is obvious that the Budapest Convention on Cybercrime, signed on 23 November 2001 and which considers cybercrime as "a threat for democracy and the states based on the rule of law", has still not been signed by Russia[55]. Numerous governments indeed consider with interest these technologies "which enable them to strike their enemies, without their legal responsibility risking being engaged with certainty"[56].

Some consider that "hybrid strategy" – as generally termed to qualify Russia's tactical methods in Ukraine – would be the "comprehensive approach gone over to the dark side of the force"[57]. In this field, as in others, everything seems to be essentially a matter of point of view. President Putin would indeed have justified Crimea's annexation in 2014 invoking the precedent of NATO's intervention in Kosovo, which was a lawful intervention but the legality of which is still disputed[58]. On the other hand, as J. Maire states, "[t]ry as hard as we may to certify that Western interventions are conditioned on

---

[50] *Ibid.*, pp. 3-4.

[51] B. Tigner, "An Evolving Threat", in *Jane's Defence Weekly*, 24 May 2017, p. 25.

[52] European Defence Agency, *Hybrid Warfare Threats – Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 November 2015 [SCS/P003198], p. 54.

[53] I. Mayr-Knoch, N. Mair and J. Mittelstaedt, "Plaidoyer pour une stratégie hybride de l'Union européenne", in *RDN*, March 2016, p. 49.

[54] *Ibid.*, p. 47.

[55] N. Arpagian, *Que sais-je ? La cybersécurité*, Paris, 2016, p. 19.

[56] *Ibid.*, p. 22.

[57] S. Biscop, "Hybrid Hysteria", in *Security Policy Brief*, No 64, June 2015, p. 1 (http://aei.pitt.edu/64790/1/SPB64.pdf);
J. Maire, "Stratégie hybride, le côté obscur de l'approche globale ?", in *RDN*, September 2016, p. 1.

[58] B. Durieux (under the direction of), *La guerre par ceux qui la font : Stratégie et incertitude au XXI^e siècle*, Monaco, 2016; A. Frachon, "Poutine, la Crimée et le Kosovo", in *Le Monde*, 27 March 2014 (https://www.lemonde.fr/idees/article/2014/03/27/poutine-la-crimee-et-le-kosovo_4390874_3232.html).

respecting international law, the quite vague interpretation of the humanitarian mandate authorising the intervention in Libya could serve as a precedent for Russia's intervention in Crimea"[59].

In any event, the concept of "hybrid strategy" initially emerged in the Western countries' general staffs and think tanks in order to define Russia's actions in Ukraine, whose goals are deemed slightly less respectable than the West's comprehensive approach[60]. The latter indeed consists in a nation "using all the military, paramilitary and non-military means at its disposal to achieve its objectives in the light of its conception of the national interest"[61]. The European Council adopted the first EU global strategy in December 2013[62] and NATO its first "Strategic Concept" in 1991[63]. Many do consider that the "Global Strategy" ("comprehensive approach"), enforced in full respect of international law, would be "the" solution in order to deal with hybrid warfare[64].

From a Western perspective, the comprehensive approach seeks to address a whole series of threats and challenges through a set of suitable and complementary means with the aim of enhancing the society's security and stability. Hybrid strategy, on the contrary, would be conceived with the aim of eroding the power of the state and influence its behaviour, with the aggressor aiming at staying below the threshold that would trigger an international reaction. Accordingly, Russia's ambition would be to attract states in its sphere of influence, using political, civil and military means in order to ensure that they would not be caught up by the Euro-Atlantic Bloc[65]. According to J. Maire, "'hybrid strategy' has become the catch-all phrase for terming the elements of power Russia used in Ukraine. It reveals in reality the West's overcompensation after years of lack of attention vis-à-vis the East, which resulted in grouping all Moscow's actions under a single term"[66].

In reality, Russia's strategic documents never mention the term "hybrid". However, the new version of the *military doctrine of the Russian Federation*, which was adopted by President Vladimir Putin on 26 December 2014, insists on the necessity, in current conflicts, to resort to other "instruments" than military power, i.e. "non-military, political, economic, informational, and other measures, that are implemented with a large use of people's inherent will to protest and special operations"[67]. Russia aspires to become again a major power in an international context where it needs to skilfully manoeuvre between its ambitions of greatness and the reality of a more and more fragile

---

[59] J. Maire, "Stratégie hybride, le côté obscur de l'approche globale ?", in *RDN*, September 2016, p. 2.

[60] *Ibid.*, p. 1.

[61] E. Tenenbaum, "Le piège de la guerre hybride", in *Focus stratégique* No 63, October 2015, p. 36.

[62] European Commission, Joint Communication to the European Parliament and the Council: "The EU's comprehensive approach to external conflict and crises", 11 December 2013 [JOIN (2013) 30 final] (https://eur-lex.europa.eu/legal-content/ga/TXT/?uri=CELEX:52013JC0030). During the post-9/11 wars, Western armed forces realised they had difficulties in managing the civilian aspect of conflicts and consequently adopted a global strategy (J. Maire, "Stratégie hybride, le côté obscur de l'approche globale ?", in *RDN*, September 2016, p. 1).

[63] NATO Press Release, *The Alliance's New Strategic Concept, agreed by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Rome on 7–8 November 1991*, NATO's Office of Information and Press, Brussels, November 1991, §24 (https://www.nato.int/cps/em/natohq/official_texts_23847.htm).

[64] United States Army Special Operations Command, *Counter-Unconventional Warfare: White Paper*, 2014, p. 9; J. Clech, "L'hybridité : nouvelles menaces, inflexion stratégique ?", in *RDN*, March 2016, p. 12.

[65] J. Maire, "Stratégie hybride, le côté obscur de l'approche globale ?", in *RDN*, September 2016, pp. 1-2.

[66] *Ibid.*, p. 3.

[67] F. d'Alançon, *Russie : la nouvelle doctrine militaire de Poutine* (www.la-croix.com), 27 December 2014.

economy. The use of hybrid strategies seems indeed to satisfy these conditions: the price remains bearable, despite potential international sanctions[68].

Russia's new strategic doctrine largely draws its inspiration from the article published in February 2013 by General Valery Gerasimov, the Russian Chief of Defence. In this document, called "Gerasimov's doctrine"[69] by some, the Chief of the General Staff of the RFAF draws the lessons from the recent Russian interventions in Estonia (2007) and in Georgia (2008)[70]. For Gerasimov, alluding in the beginning of his analysis to the "colour revolutions"[71] following the "Arab Spring", "the role of non-military means of achieving political and strategic goals has grown and, in many cases, they have exceeded the power of force of weapons in their effectiveness"[72]. At the core of its article, inspired by the recent Russian interventions in Eastern Europe, Gerasimov gives a detailed overview of the importance of non-military methods to resolve interstate conflicts, e.g. economic sanctions, political and diplomatic pressure, organising political opposition, or "disinformation"[73]. Indeed, according to him, "the information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy"[74].

The next section of this study aims to analyse the semantic complexity of "hybridity" through the official texts of the EU and NATO, but also to better understand the role played by Russia in the construction of this concept.

---

[68] G. Lasconjarias, "À l'Est du nouveau ? L'OTAN, la Russie et la guerre hybride", in *Stratégique*, No 111, Paris, 2016, p. 115.

[69] T. Selhorst, "Russia's Perception Warfare. The Development of Gerasimov's Doctrine in Estonia and Georgia and its Application in Ukraine", in *Militaire Spectator*, No 4, 2016, p. 150.

[70] *Ibid.*, p. 148.

[71] The colour revolutions refer to the popular uprisings, most of them being peaceful and supported by the West, which caused government changes in North Africa and the Middle East, but also in Eurasia (Georgia, Ukraine, Kyrgyzstan and Belarus) in the early 2000s ("The Value of Science is in the Foresight. New Challenges Demand. Rethinking the Forms and Methods of Carrying out Combat Operations", in *Military Review*, January-February 2016, pp. 24 and 29 https://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf; B. Pétric, "À propos des révolutions de couleur et du soft power américain", Hérodote, vol. 2, No 129, 2008, pp. 7-20). In May 2014, Russian Minister of Defence Sergei Shoigu denounced these colour revolutions as destabilising factors (Sergei Shoigu, *Speech at the Third Moscow Conference on International Security (MCIS)*, 22-23 May 2014).

[72] "The Value of Science is in the Foresight. New Challenges Demand. Rethinking the Forms and Methods of Carrying out Combat Operations", in *Military Review*, January-February 2016, p. 24.

[73] *Ibid.*, p. 28. "*Disinformation*" consists, through targeted social media campaigns, to manipulate information with the aim of radicalising individuals, destabilising society and controlling the political narrative (European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", 6 April 2016 [JOIN (2016) 18 final], p. 5, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en).

[74] "The Value of Science is in the Foresight. New Challenges Demand. Rethinking the Forms and Methods of Carrying out Combat Operations", in *Military Review*, January-February 2016, p. 27.

EU and NATO definitions

2010-2015: development of the concept within NATO

Although the notion of hybrid warfare, sometimes also called "non-linear warfare"[75], "unrestricted warfare"[76], "ambiguous warfare"[77], "threshold warfare"[78], or "compound warfare"[79], has been sparking off the debate for about fifteen years, particularly in the academic world, the EU and NATO definitions in this matter are quite recent. Moreover, NATO seems to have preferred since 2014 the expressions "hybrid warfare" or "hybrid warfare practices" to "hybrid threats". Finally, although the definitions proposed by the EU clearly enter into the previously described "full spectrum" school of thought, NATO's definitions have been referring, up until the Ukrainian crisis, to the kinetic school.

In an August 2010 note, NATO defined for the first time "hybrid threats" as threats "posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives"[80]. The first appearance of this concept within NATO is probably linked to General Mattis' presence in the organisation, who became in 2007 Commander for Transformation (SACT) and sought to anticipate the Atlantic Alliance's future military challenges, in the context of Russia's interventions in Estonia and in Georgia[81]. It should nevertheless be noted that, contrary to Estonia, Georgia is neither member of the EU nor NATO.

As for the document *NATO 2020: Assured security; dynamic engagement*, prepared by a group of experts on the occasion of the NATO Lisbon Summit in November 2010, it is limited to mentioning the existence of "hybrid variations that combine, for example, the stealth of a terrorist group with the

---

[75] H. Gardner, "Hybrid Warfare: Iranian and Russian Versions of 'Little Green Men' and Contemporary Conflict", in *Research Paper NATO Defense College*, Rome, No 123, December 2015, p. 1.

[76] According to Chinese Colonels Q. Liang and W. Xiangsui, "[Today,] the arena of war has expanded, encompassing the [security,] political, economic, diplomatic, cultural, and psychological spheres, in addition to the land, sea, air, space, and electronics spheres […]". These hostile acts thus flood new domains outside the classical war sphere, hence the adjective used in the title "*unrestricted (warfare)*" (Q. Liang and W. Xiangsui, *Unrestricted warfare*, Foreign Broadcast Information Service, 1999, available on http://www.cryptome.org/cuw.htm). According to Christian Malis, the book by the aforementioned two colonels, published in Chinese in 1999, is the first manifesto on hybrid warfare (Ch. Malis, "Guerre hybride et stratégies de contournement", in *RDN*, March 2016, p. 25).

[77] J. Henrotin, "La guerre hybride comme avertissement stratégique", in *Stratégique*, No 111, Paris, 2016, p. 20. The "ambiguous warfare" is associated with the question of the "attribution", i.e. the fact of not being able to determine the author of an attack (European Defence Agency, *Hybrid Warfare Threats – Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 November 2015 [SCS/P003198], p. 25).

[78] "Threshold warfare" enables to generate strategic effects without having to undergo the consequences of a military operation in due form (J. Henrotin, "La guerre hybride comme avertissement stratégique", in *Stratégique*, No 111, Paris, 2016, p. 20).

[79] According to the terminology proposed by the American historian Thomas Huber in 2002, compound warfare is a combination of a regular offensive force with an irregular force intended to destabilise the adversary. Some also talk about a "proxy war" (E. Tenenbaum, "La manœuvre hybride dans l'art opératif", in *Stratégique*, No 111, Paris, 2016, pp. 49 and 51).

[80] See SHAPE (Supreme Headquarters Allied Powers Europe) and SACT (Supreme Allied Commander Transformation) joint communication: "BI-SC Input to a new NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats", 25 August 2010 (http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf).

[81] E. Tenenbaum, "Guerre hybride : concept stratégique ou confusion sémantique ?", in *RDN*, March 2016, p. 32.

power normally associated with a nation-state, including [...] weapons of mass destruction"[82]. It is surprising to observe the absence of the term "hybrid" in NATO's latest "Strategic Concept", which was communicated during this very Summit[83].

For some experts, the 2014 Ukrainian crisis is a major strategic change in the international order[84]. The Atlantic Alliance denounces Russia's policy in this region, calling it a threat against the Euro-Atlantic security, even if – should it be recalled – Ukraine is neither member of the EU nor NATO[85]. Former NATO Secretary General Anders Fogh Rasmussen indeed assures that Russia's ambitions go beyond Ukraine, and Russia could attack a Baltic state in order to test the West's solidarity[86]. Western criticisms were at that time based on the violation of Crimea's territorial integrity and the destabilisation of eastern Ukraine, but also on the non-compliance with international law provisions[87]. NATO then decided to freeze cooperation in common projects with Russia while maintaining consultations at an ambassadors and high-level military channels scale, in order to avoid misunderstandings[88]. Moreover, the Russian-Ukrainian crisis prompted NATO and EU Member States to engage in a heavily broadcast military and security reassurance process, including the reminder of the solidarity principle enshrined in Article 5 of NATO Treaty, the building of new multinational headquarters, the setting-up of exercises and manoeuvres in Central and Eastern European countries as well as in the Black Sea, and national decisions on new military acquisitions and related larger defence budgets[89]. In this context of international tensions, the text of the 2014 Wales Summit Declaration briefly mentions the importance for NATO to be able "to effectively address the specific challenges posed by hybrid warfare threats, where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design"[90]. It is interesting to note that this definition has come closer to the "full spectrum" trend since then. As of spring 2014, the then NATO

---

[82] NATO Press Release, *NATO 2020: Assured security; dynamic engagement. Analysis and recommendations of the group of experts on a new strategic concept for NATO*, p. 17 (https://www.nato.int/cps/en/natohq/official_texts_63654.htm).

[83] NATO's Strategic Concept 2010 (https://www.nato.int/cps/fr/natohq/topics_82705.htm?selectedLocale=en).

[84] Interview by Captain-commandant (OF3) E. Hoorickx with NATO International Staff members and European External Action Service officials during the debate dedicated to the theme "*Défense européenne et OTAN: mariage de raison ?*" (European Defence and NATO: a marriage of convenience?) which took place on 29 May 2017 at the Palais des Académies in Brussels.

[85] A. Dumoulin, "Crise russo-ukrainienne. Conséquences sur les politiques de défense OTAN, UE et de défense nationale", in *Sécurité & Stratégie* (RHID), No 125, June 2016, p. 8.

[86] *Ibid.*, p. 21.

[87] Western criticisms were based on the following observations: non-compliance with the Budapest Memorandum on Security Assurances, in virtue of which Ukraine gave up nuclear weapons in exchange for the guarantee of its territorial integrity by the United States, the United Kingdom… and Russia (1994); non-compliance with the Russian-Ukrainian Friendship Treaty, according to which the Parties assure to respect each other's territorial integrity and reaffirm the inviolability of the borders existing between them (1997); breach of the principle of inviolability of frontiers (Helsinki Final Act and 1997 NATO-Russia Founding Act) (A. Dumoulin, *op. cit.*, pp. 8 and 22).

[88] A. Dumoulin, *op. cit.*, p. 8.

[89] For more details on military and security measures taken by the EU and NATO in the aftermath of the Russian-Ukrainian crisis, see A. Dumoulin, *op. cit.*, pp. 20-36; NATO Press Release, *Warsaw Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016*, § 37e and 40 (https://www.nato.int/cps/en/natohq/official_texts_133169.htm).

[90] NATO Press Release, *Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*, 5 September 2014, § 13 (https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en).

Secretary General Anders Fogh Rasmussen has been using several times the term "hybrid warfare" to describe what seems to be "a modern kind of warfare", with multiple facets and designations[91].

The text prepared by NATO Ministers of Defence on 25 June 2015 encourages an effective response of the Atlantic Alliance to "hybrid threats", but without defining its scope, and recommends, at the EU's request[92], close coordination with the European Union in this field[93]. Is it possible that the American influence is at the origin of the semantic uncertainty about the concept? The US Department of Defense indeed recently declared that it does not intend to publish a hybrid warfare doctrine, arguing that this category is too "diverse"[94]. By the way, the term "hybrid" does not appear in any of the last three US national security strategies (2006, 2010 and 2015)[95]. A 2014 US Special Forces document nevertheless defines "hybrid warfare" as "involv[ing] a state or state-like actor's use of all available diplomatic, informational, military, and economic means to destabilize an adversary"[96]. According to this document, Russia, Iran, China and the so-called "Islamic State" use hybrid methods[97].

Shortly after the terrorist attacks in Paris in November 2015, NATO proposed a strategy against "hybrid warfare", which is based on a 2015 Political Guidance and a general report on hybrid warfare endorsed by the Ministers of Defence in June 2015. It was approved by the Ministers of Foreign Affairs in December 2015 and was the subject of an "implementation plan" in February 2016. This strategic document offers a very precise definition of "hybrid warfare": "hybrid warfare is underpinned by comprehensive hybrid strategies based on a broad, complex, adaptive and often highly integrated combination of conventional and unconventional means, overt and covert activities, by military, paramilitary, irregular and civilian actors, which are targeted to achieve (geo)political and strategic objectives. They are directed at an adversary's vulnerabilities, focused on complicating decision making and conducted across the full DIMEFIL spectrum in order to create ambiguity and denial. Hybrid strategies can be applied by both state and non-state actors, through different models of engagement, which may vary significantly in sophistication and complexity. Adversaries employing hybrid strategies will seek to remain ambiguous, claim pursuit of legitimate goals and aim to keep their activities below a threshold that results in a coordinated response from the international community. This includes avoiding direct military confrontation, if possible; although the use of overt military action as part of a hybrid strategy cannot be discounted"[98].

---

[91] Anders Fogh Rasmussen, *Future NATO*, London, 19 June 2014 (https://www.nato.int/cps/en/natohq/opinions_111132.htm).

[92] European Defence Agency, *Hybrid Warfare Threats – Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 November 2015 [SCS/P003198], p. 22.

[93] NATO Press Release, *Statement by NATO Defence Ministers*, 25 June 2015, § 7 (https://www.nato.int/cps/en/natohq/news_121133.htm).

[94] L. Henninger, "La 'guerre hybride' : escroquerie intellectuelle ou réinvention de la roue ?", in *RDN*, March 2016, p. 51.

[95] J.J. Andersson and Th. Tardy, "Hybrid: What's in a Name?", in *Brief Issue* No 32, October 2015, p. 2 (https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_32_Hybrid_warfare.pdf).

[96] United States Army Special Operations Command, *Counter-Unconventional Warfare White Paper*, 2014, p. 3 (see https://publicintelligence.net/usasoc-counter-unconventional-warfare/).

[97] *Ibid.*, pp. 3, 4, 29 and 32.

[98] During the conference "Modeling and Simulation for Hybrid Environments" organised in Bucharest by the NATO Modeling and Simulation Group (NMSG) on 21-22 October 2016, the definition of "hybrid warfare" as proposed by NATO in November 2015 was mentioned (The content of this conference is available on https://www.sto.nato.int/publications/).

Interestingly enough, the definition of "hybridity" nowadays includes "non-state actors". This new semantic nuance makes it possible to consider terrorist organisations, and in particular the Islamic State, as actors of "hybrid warfare practices". However, for NATO, Moscow still seems to be the principal actor of hybrid warfare. Indeed, the "Islamic state" would also use certain hybrid practices, but without having – contrary to Russia – sophisticated power structures, including an established diplomatic network. The complexity of hybrid wars is such that only an individualised approach enables to deeply understand Russia's or the Islamic State's specificity in this field[99]. Yet the question remains whether we really can talk about "war" with "Daesh". In legal terminology, the armed attacks by this organisation against NATO countries fall indeed more within the concept of "terrorist acts"[100] in a rule of law. It would also be more appropriate to talk about "non-international armed conflict"[101], or even "civil war"[102], for terming the armed struggle which is waged by Iraq and Syria against the "Islamic State" and joined in by an international coalition as well as, formally, by NATO in May 2017[103]. In two letters addressed to the United Nations Secretary-General and to the President of the UN Security Council, Iraqi authorities indeed asked the member states to help them in the fight against IS by providing them for instance military training and air cover. Even if this request for assistance is a sufficient legal basis for the participation of the coalition in Iraq against "Daesh", the intervention is far more controversial on Syrian territory[104].

NATO further points out that "the use of hybrid strategies in conflict are [*sic*] not new, but what is new for NATO is the way a wide range of political, civil and military instruments are combined and coherently applied, aiming at particular vulnerabilities of targeted nations and international organizations in order to achieve strategic objectives"[105]. In its document called *Modeling and*

---

[99] K. Giles, "Conclusion: Is Hybrid Warfare really New?", in G. Lasconjarias and J. A. Larsen (under the direction of), *NATO's Reponse to Hybrid Threats*, forum paper 24, NATO Defence College, Rome, 2015, p. 323 (https://www.files.ethz.ch/isn/195405/fp_24.pdf).

[100] According to NATO's definition, "terrorism" means "the unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives" (*NATO glossary of terms and definitions (English and French)*, AAP-6 (2010), p. 2-T-5).

[101] A "non-international armed conflict" opposes the "armed forces [of a sovereign state] and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of [the] territory [of the above-mentioned sovereign state] as to enable them to carry out sustained and concerted military operations" (*Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II)*, 8 June 1977, article 1, http://www.un.org/ar/preventgenocide/rwanda/text-images/Geneva_Protocol2.pdf).

[102] According to the Collins dictionary, a "civil war" is "a war which is fought between different groups of people who live in the same country". A more complete definition is given by the Belgian Royal Military Academy's *Dictionnaire militaire*, according to which a civil war is a "*conflit armé important et durable qui oppose, sur le territoire d'un État, soit des groupes armés entre eux soit un ou plusieurs groupes armés au pouvoir en place. Pour qu'il y ait guerre civile proprement dite, ces groupes armés doivent être essentiellement composés de citoyens de cet État*" ("A civil war is a major and lasting armed conflict opposing, on the territory of a state, either armed groups against each other, either one or several armed groups against the regime in place. In a proper civil war, these armed groups have to be essentially composed of citizens of that state"). (*Dictionnaire militaire. Document de travail de l'École royale militaire et du Centre linguistique*, Brussels, 2005, p. 212).

[103] S.n., "L'Otan va rejoindre la coalition anti-EI", in *Le Figaro*, 24 May 2017 (http://www.lefigaro.fr/flash-actu/2017/05/24/97001-20170524FILWWW00302-l-otan-va-rejoindre-la-coalition-anti-ei.php).

[104] C. Remy, "Quel cadre légal pour la lutte armée contre l'État Islamique ?", e-Note 22 (RHID), 22 September 2016 (http://www.rhid.be/website/images/livres/enotes/E-note22.pdf).

[105] See content of the conference "Modeling and Simulation for Hybrid Environments" organised in Bucharest by the NATO Modeling and Simulation Group (NMSG) on 21-22 October 2016.

Simulation for Hybrid Environments, NATO also mentions some "modern hybrid warfare scenarios" that are "broader than just a military threat", i.e. cyber attacks, propaganda and misinformation campaigns, as well as targeted and coordinated political and economic pressure[106]. It is therefore obvious that hybrid scenarios can differ from one conflict to another and that – on a case-by-case basis – they are not necessarily illegal. Nevertheless, when applied jointly, these scenarios are more likely to threaten an allied country, or even the whole Atlantic Alliance.

Finally, following the EU's request – expressed in its April 2016 Communication – to reinforce cooperation with NATO in its fight against "hybrid threats", the Heads of State and Government reminded at the NATO Warsaw Summit in July 2016 that they "[a]greed [in December 2015] a strategy on NATO's role in Countering Hybrid Warfare, which is being implemented in coordination with the EU"[107].

Although NATO's Strategic Concepts do not mention the issue of "hybridity", they have been identifying, since the end of the Cold War, new risks threatening the Euro-Atlantic peace and stability[108]. These risks include terrorism, ethnic conflicts, disruption of the flow of vital resources, proliferation of weapons of mass destruction, but also cyber attacks, as specified in the 2010 Strategic Concept. This issue has been widely publicised since Estonia and Georgia were victims of that kind of attacks some years before. All the security challenges identified in NATO's Strategic Concepts have actually encompassed all "hybrid warfare practices" specified in the other NATO official documents since 2010. These issues call for new responses, such as the partnership with United Nations, the European Union and Russia, or the "crisis management", which are likely to affect the Atlantic Alliance's security[109].

NATO has also recommended, since the end of the Cold War, to adopt a "comprehensive approach" to effectively achieve its fundamental security tasks[110]. This strategy "recognises the importance of political, economic, social and environmental factors in addition to the indispensable defence dimension"[111]. Ultimately, the Atlantic Alliance has been aware since 1991 that it also should be able to respond to non-military security challenges, the effects of which could destabilise the organisation as much as – and sometimes even more than – a conventional military attack.

However, J. Henrotin is critical of the implementation of NATO's comprehensive – or "*intégrale*" (overall), as he puts it[112] – strategy, which too often seems to be "*séquentielle*" (sequential)[113]. He indeed considers that "the [Atlantic] Organisation as well as its member countries

---

[106] *Ibid.*

[107] NATO Press Release, *Warsaw Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016*, § 37 (i).

[108] The 1999 and 2010 Strategic Concepts are available for consultation respectively on https://www.nato.int/cps/en/natolive/official_texts_27433.htm?selectedLocale=en and https://www.nato.int/cps/fr/natohq/topics_56626.htm?selectedLocale=en. For the 1991 strategic document, see *The Alliance's New Strategic Concept, agreed by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Rome on 7–8 November 1991*, NATO's Office of Information and Press, Brussels, November 1991 (https://www.nato.int/cps/em/natohq/official_texts_23847.htm).

[109] E. Hoorickx, "Stratégie atlantique et position de la Belgique dans la 'détente' (1954-1972)", in *Stratégique*, No 110, December 2015, p. 80.

[110] See § 23 of the 1991 Strategic Concept, § 25 of the 1999 Strategic Concept and § 21 of the 2010 Strategic Concept.

[111] See § 25 of the 1999 Strategic Concept.

[112] J. Henrotin, *Techno-guérilla et guerre hybride. Le pire des deux mondes*, Paris, 2014, p. 331.

[113] J. Henrotin, "La guerre hybride comme avertissement stratégique", in *Stratégique*, No 111, Paris, 2016, p. 30.

have never been able to proceed to the concentration of military, economic or political forces necessary to the success of the adopted strategy"[114]. According to him, NATO was not able, both in the Afghanistan counter-insurgency as in the case of Ukraine, to adapt conceptually and to understand that the strategy is not only military *stricto sensu*[115]. Finally, in his opinion, NATO excessively focuses on "classic strategic concepts, i.e. a regular warfare using a kinetic mode of engagement in terms of general military strategy, which is inferior to the overall strategy mode"[116].

Hew Strachan follows Henrotin's reasoning. He indeed emphasises the existence of the conflation within NATO between "grand strategy" (political and military purposes and means to be implemented in the long term) and "military strategy" (operational plans aiming to solve specific situations in a near future)[117]. He explains the current situation through the Cold War's impact. At that time, the geographic zone of the threat was clearly defined, so that NATO's strategy could be conceived in the long term and rely on a nuclear planning[118]. According to him, [NATO's] "grand strategy" can no longer rely on a nuclear planning that is not a sufficient response to this new type of continuously more numerous and complex threats. Strachlan adds that, therefore, [NATO's] "grand strategy" now needs to be more "flexible" and in a position to apprehend unforeseen situations ("contingency") as well as what he calls "strategic shocks", i.e. the new threats emerging in the short term[119]. Nevertheless, the supreme guarantee of NATO member countries' security has always been ensured by the Alliance's – in particular the USA's – strategic nuclear forces since 1991[120]. A few years ago, the discussion about reducing the role of nuclear weapons has been addressed within NATO, with former President Barack Obama's support, who advocated a "nuclear-free world" as of 2009, but the subject was dropped after the Malaysia Airlines Boeing crash above Ukraine in July 2014[121]. . Moreover, during the NATO Warsaw Summit in July 2016, it was pointed out that "[t]he strategic forces of the Alliance, particularly those of the United States, are the supreme guarantee of the security of the Allies"[122].

The issue of "hybrid threats" and the strategy to respond to it appeared later in the European circles.

An issue at the heart of the European security policy since 2015

Since F. Mogherini took up her office as High Representative of the European Union for Foreign Affairs and Security Policy in November 2014, but also after the upsurge of Islamist terrorism in Europe and following the Ukrainian crisis, the EU has indeed intended to make fighting against

---

[114] *Ibid.*, p. 28.

[115] *Ibid.*

[116] J. Henrotin, "L'hybridité à l'épreuve des conflits contemporains : le cas russe", in *RDN*, March 2016, p. 40.

[117] E. Hoorickx, "Stratégie atlantique et position de la Belgique dans la 'détente' (1954-1972)", in *Stratégique*, No 110, December 2015, p. 81.

[118] *Ibid.*, p. 80.

[119] *Ibid.*, p. 81.

[120] See § 55 of the 1991 Strategic Concept, § 62 of the 1999 Strategic Concept and § 18 of the 2010 Strategic Concept.

[121] Interview with R. Huygelen (Belgian Ambassador to NATO from 2010 to 2014), by Captain-commandant (OF3) E. Hoorickx on 16 July 2015.

[122] NATO Press Release, *Warsaw Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016*, § 53.

"hybrid threats" one of its priorities[123]. Before that, the hybridity issue was not mentioned in the official European documents. In February 2015, i.e. one month after the *Charlie Hebdo* shooting, the EU Defence Ministers informally met in Riga in order to discuss current issues and prepare the European Council meeting on defence in June 2015. On that occasion, they discussed the EU response to "hybrid threats" and stressed the need for closer EU-NATO cooperation in this regard[124].

Following this Riga meeting, the European External Action Service (EEAS) defined for the first time the term "hybrid warfare" in May 2015. The then prevailing international situation was particularly worrying, especially in Ukraine and Europe, where deadly terrorist attacks claimed by "Daesh" had been carried out. Having drawn its inspiration from the "hybrid warfare" definition provided by NATO in 2014 during the Wales Summit, the EU offered more explanations on the operating modes that the adversary can resort to in the context of a "hybrid war", as well as on its Member States' "weaknesses" against "hybrid attacks". The EEAS defines "hybrid warfare" as "a centrally designed and controlled use of various covert and overt tactics, enacted by military and/or non-military means, ranging from intelligence and cyber operations through economic pressure to the use of conventional forces. […] [T]he attacker seeks to […] destabilise an opponent by applying both coercive and subversive methods. The latter can include various forms of sabotage, disruption of communications and other services including energy supplies. The aggressor may work through or by empowering proxy insurgent groups, or disguising state-to-state aggression behind the mantle of a 'humanitarian intervention'. Massive disinformation campaigns designed to control the narrative are an important element of a long-term hybrid campaign. All this is done with the objective of achieving political influence, even dominance over a country in support of an overall strategy."[125] Furthermore, an important aspect of hybrid warfare is to generate ambiguity amongst the population and the international community. Indeed, ambiguity, i.e. the problem of an incomplete "attribution", prevents a rapid and effective response, since it becomes difficult to know who is behind an attack[126]. This reflection has probably contributed to the creation of a new concept, namely "ambiguous warfare", which many researchers associate with Moscow's recent interventions in Ukraine. Finally, according to the European Defence Agency, the fundamental characteristic of a "hybrid attack" is that it aims to exploit a state's "vulnerabilities", and these weaknesses – such as the difficulty to implement an effective strategic communication or to protect critical infrastructures – vary depending on the Member States and are linked to weaknesses inherent to certain structurally decentralised Western democracies[127].

In June 2015, the High Representative, who then "took for granted an [unspoken] definition of hybrid threats"[128], asked the European Parliament and the Council to improve the relevant knowledge

---

[123] European Defence Agency, *Hybrid Warfare Threats – Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 November 2015 [SCS/P003198], pp. 21-22.

[124] A. Gnēze, "Media release. EU Defence Ministers in Riga call for unity in addressing European security threats", 19 February 2015 (https://eu2015.lv/news/media-releases/666-eu-defence-ministers-in-riga-call-for-unity-in-addressing-european-security-threats).

[125] European Defence Agency, *op. cit.*, p. 21.

[126] European Defence Agency, *Hybrid Warfare Threats – Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 November 2015 [SCS/P003198], pp. 20, 25 and 26.

[127] *Ibid.*, p. 54.

[128] *Ibid.*, p. 22.

and to strengthen the EU's "resilience"[129] as well as its cooperation with NATO in this field[130]. At that time, P. Pawlak, researcher at the European Parliament, identified some very diverse examples of "hybrid threats": terrorism, deficient cyber security, organised crime, maritime disputes, space issues, resource scarcity, and "covert operations", such as Russia's use of special forces (i.e. "green men") and information warfare in Ukraine[131]. According to his analysis, a "hybrid threat" would be associated with a specific operating mode, even though hybridity, by definition, can only designate a "combination of two"[132].

In October 2015, the EU Military Staff also presented a definition of "hybrid warfare" as the "combined, centrally designed and controlled use of various covert and overt activities, ranging from conventional forces, through economic pressure to intelligence"[133]. It added that disinformation campaigns as well as coercive and subversive tactics are at the heart of hybrid strategy, which ultimately consists in "the offensive use of a comprehensive array of instruments (e.g. political, ideological, economic, informational, humanitarian etc.) in conventional and unconventional ways against a state"[134].

Finally, the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication of 6 April 2016 proposed a new explanation for "hybrid threats", largely based on the definitions proposed by the EU and then by NATO in 2015. According to this Joint Communication, the concept of "hybrid threats" aims to capture a "mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats"[135]. This document also specifies that "definitions of hybrid threats vary and need to remain 'flexible' to respond to their evolving nature"[136].

The semantic explanation for hybrid threats proposed in the Joint Communication gives rise to two reflections. On the one hand, it suggests that a "hybrid threat" corresponds to a specific operating mode, which – as previously said – is in contradiction with the very terminology of "hybridity". On the other hand, the definition proposed by the EU on the so-called "unconventional" methods is not in line with the definition used in academic circles. Indeed, the so-called unconventional warfare is

---

[129] "Resilience is the capacity to withstand stress and recover, strengthened from challenges" (European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", 6 April 2016 [JOIN (2016) 18 final], p. 6. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en).

[130] European Council, European Council Conclusions, 25-26 June 2015 [EUCO 22/15, § 10 (c)] (https://www.consilium.europa.eu/media/21717/euco-conclusions-25-26-june-2015.pdf).

[131] P. Pawlak, *At a glance. Understanding Hybrid Threats. European Parliamentary Research Service*, https://epthinktank.eu/2015/06/24/understanding-hybrid-threats/, 24 June 2015.

[132] H. Pierre, *(Re)penser l'hybridité avec Beaufre*, *Stratégique*, No 111, Paris, 2016, p. 34.

[133] EU Military Staff, *Draft Food for Thought Paper: Possible EU Military Contributions to Countering Hybrid Threats*, 2 October 2015 [EEAS (2015) 1367 REV1], § 3.

[134] *Ibid.*

[135] European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", 6 April 2016 [JOIN (2016) 18 final], p. 2.

[136] *Ibid.*

traditionally characterised by guerrillas lead by irregular armed groups with light weapons and a very limited technological level. According to this terminology, diplomacy or economics are therefore not part of unconventional warfare. "Unconventional methods", to which the Joint Communication of 6 April 2016 makes reference, rather seem related to operating modes that are not specifically military.

In order to counter "hybrid threats", the EU recommends, inter alia, that "resilience" to both cyber attacks and terrorist or criminal acts be strengthened[137]. The Joint Communication nevertheless states that "[a]lthough terrorist acts and violent extremism are not per se of a hybrid nature, perpetrators of hybrid threats can target and recruit vulnerable members of society, radicalising them through modern channels of communication (including internet social media and proxy groups) and propaganda"[138]. This consideration accordingly implies that terrorism and organised crime are "hybrid threats" only when their perpetrators use disinformation and propaganda. Indeed, according to a member of the EU INTCEN (European Union Intelligence and Situation Centre), "a terrorist attack or organised crime activities are hybrid threats only if they are resorted to in order to obtain political results that would not be obtained through the [conventional] military way"[139]. This person adds that "the Paris attacks in November 2015 are [therefore] not a hybrid threat, [as their authors did not have another objective than bringing terror]"[140]. In order to talk about "hybrid threats", there needs to be "not only the use of certain hybrid tools, but also the intention to pressure a state in order to obtain military results through means which are not directly military"[141].

Although the first EU strategic documents did not mention the term "hybrid", they nevertheless identified the same security threats than the ones mentioned in NATO's "Strategic Concepts", such as terrorism, organised crime, proliferation of weapons of mass destruction[142] or, as of 2013, the "degradation of resources" and cyber security[143]. Indeed, that year began what would become the "Snowden Affair", named after Edward Snowden, a former IT engineer at Booz Allen Hamilton, subcontractor for the National Security Agency (NSA). Snowden disclosed the existence of "PRISM", a large-scale spy programme lead since 2007 by the NSA outside U.S. territory[144]. The German weekly magazine *Der Spiegel* indeed revealed, in October 2013, that German Chancellor Angela Merkel's

---

[137] *Ibid.*, pp. 11 and 15.

[138] *Ibid.*, p. 15.

[139] Interview at the EU INTCEN by Captain-commandant (OF3) E. Hoorickx, 30 November 2016.

[140] *Ibid.*

[141] *Ibid.*

[142] Although the issue of the proliferation of weapons of mass destruction is widely addressed in the EU 2003 Strategic Concept, it is surprisingly not mentioned in the 2016 Strategic Concept (Note of the EU's High Representative, A secure Europe in a better world – European security strategy, Brussels, 12 December 2003, pp. 3-4, http://data.consilium.europa.eu/doc/document/ST-15849-2003-INIT/en/pdf); European Commission, Joint Communication to the European Parliament and the Council: "The EU's comprehensive approach to external conflict and crises", 11 December 2013 [JOIN (2013) 30 final] (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0030&qid=1542718671190&from=EN).

[143] Note of the EU's High Representative, A secure Europe in a better world – European security strategy, Brussels, 12 December 2003; European Commission, Joint Communication to the European Parliament and the Council: "The EU's comprehensive approach to external conflict and crises", 11 December 2013 [JOIN (2013) 30 final], pp. 2 and 4.

[144] N. Arpagian, *Que sais-je ? La cybersécurité*, Paris, 2016, p. 3.

personal mobile phone has been listened in on by "big American ears".[145]. The EU's new Strategic Concept of 2016, still applicable, included the issue of "hybrid threats" for the first time[146].

Nowadays, hybrid threats are still a major concern for political decision-makers. Recently, Guy Verhofstadt, president of the Alliance of Liberals and Democrats for Europe, insisted on Europe's need to resist to "the hybrid warfare that Putin wages on the West". He considers that, "through disinformation sites and cyber attacks, Russia [indeed] seeks to undermine Europeans' faith in democracy"[147]. He is here referring to the cyber operation ascribed to Russia on the occasion of the U.S. presidential elections, the hack on the German Bundestag in early 2015, the cyber attack suffered by the European Commission in November 2016, and Russia's financial support to European far-right nationalist organisations and populist movements, in particular during the major elections in 2017[148].

Ultimately, although "hybrid threats" have been at the heart of the EU and NATO's strategy, especially since the beginning of the Ukrainian crisis, a certain semantic confusion still exists. The concept of "hybrid warfare" is as a matter of fact far from winning unanimous support. Concerns indeed exist about the relevance, usefulness and reasons of using such a terminology.

"Hybrid warfare": "intellectual swindle"[149] or "occasion to look contemporary conflictuality in the eye"[150]?

The concept of "hybrid warfare" is the subject of much debate[151] and even sometimes causes controversy. Accordingly, for some researchers such as Gérard Chaliand, this term "hardly helps to understand the phenomenon. It is more about irregular warfare where guerrilla meets terrorism and all old and new means (including at communication level and in the field of drugs)"[152]. He also states that "the invention of new words to term a known phenomenon hardly helps to improve the capacity to define a proper response"[153]. Laurent Henninger even considers that the debate on "hybrid warfare" proceeds from a "reinvention of the wheel", or is even an "intellectual swindle"[154]. He indeed thinks that no "hybrid" particularity is really new nor, above all, justifies a new characterisation of warfare,

---

[145] *Ibid.*, p. 4.

[146] Note from the General Secretariat of the Council of the European Union, A Global Strategy for the European Union's Foreign and Security Policy, 28 June 2016 [EU's comprehensive approach, December 2013, PESC 543, PSDC 395], p. 16 (http://data.consilium.europa.eu/doc/document/ST-10715-2016-INIT/en/pdf).

[147] G. Verhofstadt, "Résistons à la guerre hybride que Poutine mène contre l'Occident", in *Le Monde*, 2 January 2017 (http://www.lemonde.fr/idees/article/2017/01/02/resistons-a-la-guerre-hybride-que-poutine-mene-contre-l-occident_5056270_3232.html).

[148] *Ibid.*

[149] L. Henninger, "La 'guerre hybride' : escroquerie intellectuelle ou réinvention de la roue ?", in *RDN*, March 2016, p. 51.

[150] J. Henrotin, "La guerre hybride comme avertissement stratégique", in *Stratégique*, No 111, Paris, 2016, p. 31.

[151] J.-C. Coste, "De la guerre hybride à l'hybridité cyberélectronique", in *RDN*, March 2016, p. 19.

[152] J. Henrotin, "Entretien stratégique avec Gérard Chaliand. Les mutations de la guerre irrégulière", in *Stratégique*, No 111, Paris, 2016, p. 141.

[153] *Ibid.*, p. 142.

[154] L. Henninger, "La 'guerre hybride' : escroquerie intellectuelle ou réinvention de la roue ?", in *RDN*, March 2016.

"because its extension to new dimensions, means, methods, etc. has not altered its nature"[155], He states that, "if there are some changes, these are generally changes in volume or possibly in the focus on such or such point [...]"[156]. He adds: "the problem is that, since at least the 1950s, we are obsessed by classifying wars and conflicts, [which has] quite largely contributed to spread confusion [...]"[157]. According to Henninger, the creation of a new vocable ultimately risks to introduce much confusion among military and civilian minds, "which are already on the verge of being overloaded in this matter"[158]. As for Tenenbaum, he also warns against the "hybrid warfare" concept's "plasticity"[159]. He indeed deems that it "refers to both politico-strategic and tactical-operational realities and, without an agreement between the users of this expression on the exact meaning of it, there is a good chance that it causes many misunderstandings, or even dangerous cross-purposes"[160].

According to J. Henrotin, the debate on hybrid warfare does not proceed from an "intellectual swindle", "at least, in tactical-operational terms, as the same cannot be said about the strategic aspects"[161]. He indeed points out that the various vectors of strategic interpretation as to hybrid warfare, i.e. overall strategy, proxy wars, use of irregular fighters, information warfare, but also rallying a "political rhetoric to be exempted from legal obligations or contest their significance"[162] are classic means from a historical point of view, including when they are combined[163]. During the Vietnam War, for example, irregular fighters (Vietcong) were directly armed by Hanoi and ultimately benefited from Moscow's support. Moreover, just as for Russia's intervention in Ukraine, the 1990 Kuwait invasion and the construction of artificial islands in South China Sea in order to have a much larger than initially existing exclusive economic zone recognised follow the same logic of legitimacy of action, on the basis of a "biased interpretation of international law", or even, possibly, of historical arguments[164].

According to Henrotin, the innovation would rather be [tactical-]technical[165]. He indeed considers that "the concept of hybrid warfare in tactical-operational terms [...] summarises an authentic mutation, with possibly important consequences for Western armed forces: a major qualitative leap [...]. The structures following hybrid fight lines would therefore occupy the field of particular strategies (e.g. air/airspace, naval strategies) and would be able to implement improvised chemical weaponry while enhancing their fire-power in the land domain, by developing C5I capabilities (Counter Command, Control, Communications, Computers and Intelligence) and a truly media strategy enabling them to act on a global scale"[166]. He adds that these [tactical-operational] evolutions are made possible thanks to an easy access to advanced – in particular civilian – technologies, but especially as a result of the military exploitation of these technologies through an innovation process [specific] to

[155] *Ibid.*, p. 53.

[156] *Ibid.*

[157] *Ibid.*, p. 54.

[158] *Ibid.*, p. 53.

[159] E. Tenenbaum, "Le piège de la guerre hybride", in *Focus stratégique* No 63, October 2015, p. 43.

[160] *Ibid.*

[161] J. Henrotin, "La guerre hybride comme avertissement stratégique", in *Stratégique*, No 111, Paris, 2016, p. 17.

[162] *Ibid.*, p. 26.

[163] *Ibid.*, pp. 26-27.

[164] *Ibid.*, p. 38.

[165] *Ibid.*, p. 24.

[166] *Ibid.*, pp. 17-18.

irregular fighters' organisational agility[167]. According to Tenenbaum, given the rapid spread of precision weaponry, "the surprising combinations of hybrid fight will become the standard, and the very term could seem less useful within a few years, as all irregular structures will be in possession of such means. Therefore, there is no evidence that this concept has a promising future ahead"[168].

Henrotin wrote that "the massification of the fighters' *de-identification*"[169] [observable in hybrid warfare] also represents a [tactical] break with former conflicts. The innovation of this phenomenon can be found in the action's systematic aspect and the volume of engaged forces, and not in the issue of clandestine operations, which is historically not new[170].

According to Gérard Chaliand, "the innovation [in current conflicts] [...] lies [...] in the intellectual field, the various know-hows and the psychological manipulation of the adversary – i.e. us [the Western powers] –, whereas, not so long ago, about fifty years ago, this was not the case. In olden days, any adversary knew us only very little. Nowadays, not only does he know us, but he also knows our weaknesses. The real change came with the social networks."[171] The adversary "knows, with the indirect assistance of our own media that are longing for audience rating, how to manipulate us and instil fear and psychosis[172]. I. Mayr-Knoch follows G. Chaliand's reasoning. According to him indeed, in "hybrid warfare", "incorporating the civil instruments of pressure to the military means is crucial"[173]. Russia's hybrid operations in eastern Ukraine have been impressive in this field. He therefore recommends that the EU launches a "campaign for winning hearts and minds"[174] in the Baltic States, so as to prevent Russia from being able to "repeat its dividing tactics by exploiting the existing divides between the Russian-speaking minority and the rest of the society"[175]. This is also what Tenenbaum recommends; he encourages to develop a real "political project"[176] in order to counter "hybrid methods". For example, in order to avoid that an aggression from outside coincides with an insurgency, the latter must be fought with not only military means but also mainly political means by attempting to accede, as far as possible, to the population's claims, provided that these claims are not incompatible with our fundamental interests. In his opinion, the priority should be placed on eliminating lawless areas, re-establishing a judicial and police presence on the whole territory, as well as on adopting political and social measures addressing the problems causing the conflict[177].

---

[167] *Ibid.*, p. 18.

[168] E. Tenenbaum, "Le piège de la guerre hybride", in *Focus stratégique* No 63, October 2015, p. 43.

[169] The concept of "de-identification" ("*dé-identification*") is used in a situation where an attacker is not clearly identified (J. Henrotin, "La guerre hybride comme avertissement stratégique", in *Stratégique*, No 111, Paris, 2016, p. 27).

[170] J. Henrotin, "La guerre hybride comme avertissement stratégique", in *op. cit.*, p. 26.

[171] J. Henrotin, "Entretien stratégique avec Gérard Chaliand. Les mutations de la guerre irrégulière", in *Stratégique*, No 111, Paris, 2016, p. 141.

[172] *Ibid.*, p. 142.

[173] I. Mayr-Knoch, N. Mair and J. Mittelstaedt, "Plaidoyer pour une stratégie hybride de l'Union européenne", in *RDN*, March 2016, p. 44.

[174] The expression "hearts and minds" is not new. It is attributed to Sir Gerald Templer, commanding officer of the British forces in Malaysia during the counterinsurgency in this country in 1951-1954. It refers to "all the activities and processes through which a government, a party, any constituted political entity works on inflecting the population's state of mind" (F. Géré, Dictionnaire de la désinformation, Paris, 2011).

[175] I. Mayr-Knoch, N. Mair and J. Mittelstaedt, *op. cit.*, p. 50.

[176] E. Tenenbaum, "Le piège de la guerre hybride", in *Focus stratégique* No 63, October 2015, p. 40.

[177] *Ibid.*, pp. 40-41.

In the end, J. Henrotin considers that focusing the hybridity on the Russian issue "tends to distort strategic reflection" [178] about the concept of "hybrid warfare" and prevents a sound appraisal of a complex situation[179], whereas its analysis should be an "occasion to face up to contemporary conflictuality"[180]. This view is also shared by Henninger, who recommends not to attempt to characterise with a unique and reductive adjective a number of geopolitical phenomena which should, on the contrary, be considered in all their diversity and complexity[181]. In other words, Henrotin affirms that Russia's success is much more based on the following operational military qualities (or "principles of war"[182]): security, surprise[183], concentration of forces, tempo, planning and correlation of forces, than on using hybrid means such as propaganda, or "de-identification", which is of no use to the NATO Treaty's Article 5. Indeed, "the determining point triggering the NATO Treaty's Article 5 is the attack, not whether the attacker is clearly identified or not"[184]. Accordingly, "once engaged in operations, the fighter, whether identified or not, is considered as an adversary in the light of international law, and is therefore a perfectly legitimate target […]. In this sense, the concerns highlighted by some observers on a possible use of these 'de-identified' forces against the Baltic States seem ill-founded"[185]. Consequently, making Russia a paradigm of hybrid operations amounts to "being mistaken about the nature of future operations, while reproducing the errors that make us vulnerable"[186]. Would NATO and the EU not be sufficiently aware that the current enemy is able to combine the quantity (or "fire-power" [187]) we no longer have, with the quality we think we still have? Consequently, in the case of Russia, the share of defence expenditure steadily increased between 2010 and 2015, from 12.5% of the national budget to 19.7% (and from 2.84% of the GDP in 2010 to 4% in 2014)[188]. Moreover, NATO recognises that Russia's military power is a fundamental challenge for the Atlantic Alliance[189]. It is indeed undeniable that the Russian armed forces have initiated in recent years a major modernisation and continue their rearmament with the development of their military–industrial complex under a

[178] J. Henrotin, "L'hybridité à l'épreuve des conflits contemporains : le cas russe", in *RDN*, March 2016, p. 37.

[179] J. Henrotin, "La guerre hybride comme avertissement stratégique", in *Stratégique*, No 111, Paris, 2016, p. 29.

[180] *Ibid.*, p. 31.

[181] L. Henninger, "La 'guerre hybride' : escroquerie intellectuelle ou réinvention de la roue ?", in *RDN*, March 2016, p. 55.

[182] J. Henrotin, *Techno-guérilla et guerre hybride. Le pire des deux mondes*, Paris, 2014, p. 141.

[183] André Dumoulin does not share the statement according to which NATO and its allies would have experienced a strategic surprise with Crimea's annexation. He points out that it is difficult to confirm this statement "as the Western strategic and satellite detection systems were operational, despite the fact that Russia organised the annexation by coordinating hybrid – to use a fashionable word – actions, by giving visibility to paramilitary forces and other militias of uncertain origin, resulting in the operation ending with virtually no victims" (A. Dumoulin, "Crise russo-ukrainienne. Conséquences sur les politiques de défense OTAN, UE et de défense nationale", in *Sécurité & Stratégie* (RHID), No 125, June 2016, p. 14).

[184] J. Henrotin, "La guerre hybride comme avertissement stratégique", in *op. cit.*, p. 27.

[185] *Ibid.*

[186] J. Henrotin, "L'hybridité à l'épreuve des conflits contemporains : le cas russe", in *RDN*, March 2016, p. 43.

[187] J. Henrotin, *Techno-guérilla et guerre hybride. Le pire des deux mondes*, Paris, 2014, p. 121.

[188] I. Facon, "Que vaut l'armée russe ?", in *Politiques étrangère*, vol. Printemps, No 1, 2016, p. 153.

[189] NATO Press Release, *Warsaw Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016*, § 5.

programme scheduled to be completed in 2020[190]. According to General Hans-Lothar Domröse, former Commander of Allied Joint Force Command Brunssum, Russia surpasses NATO in the military field as a result of the continual modernisation of its military equipment, which enabled Russia to develop a high combat capability, as well as the manoeuvrability and firepower of its armed forces. On the contrary, he observes that NATO troops have drastically decreased during the last 25 years. He therefore recommends that Russia and NATO start negotiations on disarmament in order to rebalance the ratio of powers[191]. However, these recent years' spiral of confrontation between NATO and Russia does not pave the way for discussions on that subject. During the Atlantic Alliance's Summits in Wales in 2014 and in Warsaw in 2016, a real NATO rearmament programme was even defined. In Warsaw, the Atlantic Alliance also put the emphasis on the need to maintain tactical nuclear forces in its aero-terrestrial plan[192]. In turn, Vladimir Putin ordered to reinforce, as from 2017, Russia's nuclear force so that it is able to break through any missile shield, such as the missile defence system Washington intends to deploy in Eastern Europe[193]. It should, however, be noted that Russia's defence budget has significantly decreased since 2016 and remains far below the United States' or China's defence budget[194].

A power such as "Daesh" has between 30,000 and 50,000 fighters[195] armed with sophisticated weapons, which is a real quantitative leap for a terrorist organisation[196]. Henrotin concludes that the technical-tactical excellence of Western countries' weapon systems is not sufficient against these new military arsenals. Tactics is truly nothing without a long-term strategy and sufficient troops provided

---

[190] S. Gilbert, "La modernisation des forces armées russes", Draft General Report of the NATO Parliamentary Assembly [064 STC 15 F], pp. 2-3. For more details on the Russian armed forces' troops and means, read: IISS, *The Military Balance 217*, London, 2017, pp. 210-223.

[191] Ch. Saarländer, "Deutscher NATO-General warnt vor russischer Militär-Überlegenheit", in *Contra Magazine*, 2 January 2016 (https://www.contra-magazin.com/2016/01/deutscher-nato-general-warnt-vor-russischer-militaer-ueberlegenheit/). There are no figures detailing systematically the military troops committed to NATO. The major streamlining of its commanding structures since the end of the Cold War nevertheless enables to have a better insight into the NATO personnel reduction.

[192] P. Quilès, "Tensions entre l'OTAN et la Russie : risque de confrontation militaire ?", in *Recherches internationales*, No 108, January-March 2017, pp. 70-72.

[193] S.n., "Russie : Poutine ordonne le renforcement de la force de frappe nucléaire", in *Le Monde*, 22 December 2016 (http://www.lemonde.fr/international/article/2016/12/22/russie-poutine-ordonne-le-renforcement-de-la-force-de-frappe-nucleaire_5052934_3210.html).

[194] In 2016, the United States' military expenditure amounted to 611 billion dollars, against 215 billion dollars for China and about 69.2 billion dollars for Russia, making it the third largest spender country in terms of military expenditure (SIPRI, "World military spending: increases in the USA and Europe, decreases in oil-exporting countries" (Press release), Stockholm, 24 April 2017, p. 1. https://www.sipri.org/media/press-release/2017/world-military-spending-increases-usa-and-europe).

[195] Figures provided by O. Saugues, "Rapport d'information sur le Proche et Moyen-Orient", in *Rapport d'information de l'Assemblée nationale*, No 2666, 18 March 2015, p. 66. As for the *Soufan Group*, an international strategic consultancy group based in New York, it estimated in December 2015 that IS had between 27,000 and 31,000 fighters, i.e. twice as many as the figure estimated in June 2013 (*SIPRI Yearbook 2016*, Oxford, pp. 28-29).

[196] Al-Qaeda would have had less than one thousand fighters in Afghanistan in the 2000s. Former French Defence Minister Jean-Yves Le Drian estimated in September 2014 that "Daesh" probably had "3,000 American 4x4 Hummers picked up in Mossul, 60,000 individual weapons, 50 heavy tanks, 150 light tanks and anti-tank materiel" (O. Saugues, "Rapport d'information sur le Proche et Moyen-Orient", in *Rapport d'information de l'Assemblée nationale*, No 2666, 18 March 2015, p. 66). Although it is difficult to assess the current weapon stockpile of Daesh, there is no evidence to establish that this terrorist organisation has bacteriological or nuclear weapons (K. Arif, "Rapport d'information sur les moyens de Daesh", in *Rapport d'information de l'Assemblée nationale*, No 3964, 13 July 2016, p. 387).

with a proper know-how. Moreover, the Western forces' overstretch, whether in internal or external operations, leads to a loss of know-how, while the potential adversary is acquiring it[197]. According to Henrotin, we are running the risk of gradually ending up with "new armed forces dating from the old order"[198], i.e. professionalised forces, technically excellent, but which could end up proving inefficient, as the forces of the former historical cycle. Tenenbaum suggests adopting a capability model adapted to the evolution and diffusion of weapon systems and non-linear tactics[199]. As for Roland Freudenstein, he insists on the need for the EU and NATO to increase their supply of trained men in order to fight against "hybrid threats", particularly in terms of disinformation. In his opinion, the EU only has about ten people, NATO hardly twice as much, to fight against Moscow's propaganda spread by some 500 experts in this field, also called "trolls". However, he adds, Russia's disinformation efforts have become much more complex than during the Cold War, where "it was just one big unitary lie; now it's a complex range of things"[200].

According to Colonel E. A. Claessen, it is not by increasing the technological lead of their armament systems that NATO countries will succeed in countering Russia's strategy. He asserts that the latter is conceived in order to neutralise the benefits that NATO draws from its state-of-the-art technology. He is convinced that "rather than developing means to destroy so-called strategic targets with increasing precision and from ever longer distances, Western countries should develop capabilities in the fields of understanding, information and influence operations, humanitarian assistance and providing of urban essential services in regions in conflict. It is the only way to prevent the adversary from relying on the population's potential for protest in view of drawing out these conflicts". He concludes that "those who only invest in wars without contact will sink everywhere into wars without victory"[201].

According to Elie Tenenbaum, the coining of the expression "hybrid warfare" – which he terms a "vague concept the specificity of which is often hard to grasp"[202] – elaborates on "the impoverishment of strategic culture in the European political circles and the unsuitability of collective defence mechanisms"[203]. He adds that "hybrid warfare" has become a "bureaucratic survival issue for many partners"[204], as can be seen from the proliferation of NATO Centres of Excellence or think tanks addressing this issue. He claims that the members of these institutions sometimes even choose to distort the concept's meaning in order to better match it with their skills. "All emerging challenges, whether military or not, have suddenly become likely to be labelled as 'hybrid threats', ranging from cyber attacks to terrorism, [...] maritime piracy, and biotechnologies"[205]. A leading figure from EU INTCEN ventures its own conception that hybrid warfare has become a central issue for NATO, with a particular

---

[197] J. Henrotin, "La guerre hybride comme avertissement stratégique", in *Stratégique*, No 111, Paris, 2016, pp. 30-31.

[198] *Ibid.*, p. 31.

[199] E. Tenenbaum, "Le piège de la guerre hybride", in *Focus stratégique* No 63, October 2015, p. 39.

[200] B. Tigner, "An Evolving Threat", in *Jane's Defence Weekly*, 24 May 2017, p. 25.

[201] E. A. Claessen, "La pensée militaire russe : 'guerre sans contact, guerre sans victoire'", in *RDN*, May 2016, p. 107.

[202] E. Tenenbaum, "La manœuvre hybride dans l'art opératif", in *Stratégique*, No 111, Paris, 2016, p. 47.

[203] E. Tenenbaum, "Le piège de la guerre hybride", in *Focus stratégique* No 63, October 2015, p. 43.

[204] *Ibid.*, p. 35.

[205] *Ibid.*

focus on Russia, a power which, in his opinion, should not be considered only as an enemy, but also as a partner[206].

According to Ch. Malis, the promotion of the hybridity concept, which "presents a [semantic] overextension and an obvious eccentric hallmark", should be understood as a political reconstruction effort of a common business plan for NATO countries at a time when its cohesion, particularly concerning the Euro-American and intra-European relations, is affected by worrisome dissensions as a result of the situation in Eastern Europe[207]. According also to Guillaume Lasconjarias, the interest of "hybrid warfare" concept is to redefine, today and for the near future, the defence strategies, but also the role and organisation of security architectures[208].

Lasconjarias also states that "this ['hybrid warfare'] term's popularity perfectly illustrates the interest of a chameleon concept which can accordingly refer to different realities, whether it be Russia on the east or a non-state armed group such as Daesh […]. [Ultimately,] hybridity appears as a comforting concept, as it makes it possible to include everything which is unconventional […]. [However, as often reminded by] Secretary General Jens Stoltenberg, […] the first form of hybrid warfare is to be found in the Trojan horse, and […] there is nothing that we have not seen or experienced before"[209]. Though, according to Lasconjarias, "hybridity sheds more light on the fragility of states dragged into a globalisation process which is going over their heads, and highlights the current policies' insufficiency to think about the world order, their place and their role. It is therefore not uninteresting to observe that the response to the various hybridity forms fits often in one other catch-all word: resilience"[210]. The next chapter considers the strategy currently proposed by the EU and NATO to face up to hybrid threats, including in terms of "resilience".

[206] Interview at the EU INTCEN by Captain-commandant (OF3) E. Hoorickx, 30 November 2016.

[207] Ch. Malis, "Guerre hybride et stratégies de contournement", in *RDN*, March 2016, p. 24.

[208] G. Lasconjarias, "À l'Est du nouveau ? L'OTAN, la Russie et la guerre hybride", in *Stratégique*, No 111, Paris, 2016, p. 117.

[209] *Ibid.*, p. 108.

[210] G. Lasconjarias, "À l'Est du nouveau ? L'OTAN, la Russie et la guerre hybride", in *Stratégique*, No 111, Paris, 2016, p. 117.

Part 2: the Euro-Atlantic Strategy against "hybrid campaigns" and Belgium's involvement in this strategy

"Hybrid warfare" practices are considered a major security challenge by the EU and NATO. Since 2015 they are bent on developing, separately, a consistent strategy in order to help their member states in the fight against this complex threat. The strategic response proposed by the EU and NATO, both wishing to cooperate on countering "hybrid campaigns", is structured around five elements: enhancing knowledge about "hybrid practices", building resilience against those practices, strengthening the efficiency of prevention and response to hybrid attacks (Integrated Political Crisis Response) and, finally, better cooperation between the EU and NATO in all those fields, as well as strategic communication and cyber security[211]. Although both organisations commit to supporting their member states in countering "hybrid campaigns", they insist that the primary responsibility lies with the member states, insofar as countering hybrid threats relates to national security and defence as well as the maintenance of law and order[212]. This part of the study aims to analyse the strategy implemented by both organisations as well as the measures taken by Belgium in order to participate in the project.

Recognising "hybrid campaigns" and determining their authors

The first EU and NATO action area covers the knowledge of "hybrid threats". Both organisations would like to be able to detect and appropriately respond to emerging hybrid threats in order to prevent a hybrid campaign from degenerating into a military conflict. The EU and NATO therefore invite their member states to identify their weaknesses – or "vulnerabilities" – in the face of hybrid risks[213]. In June 2017, the president of the European Council decided to establish a "Friends of the Presidency Group" (FoP), bringing together experts from all the EU Member States[214] and appointed until the end of June 2018, in order to help Member States to achieve this

[211] European Parliament, *Countering hybrid threats: EU-NATO cooperation*, March 2017 (http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf).

[212] European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", 6 April 2016 [JOIN (2016) 18 final], p. 2 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en); *Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers*, 11 February 2016 (https://www.nato.int/cps/en/natohq/opinions_127972.htm?selectedLocale=en).

[213] European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", 6 April 2016 [JOIN (2016) 18 final], p. 4.

[214] "FoP members are responsible for coordinating the project of identifying the Member States' critical vulnerabilities to hybrid threats. Most of them are also the contact persons entitled to represent their Member State to the EU Hybrid Fusion Cell". Telephone interview on 18 August 2017 with E. Lallemant, Permanent Representative of Belgium to the EU and Belgium's contact person to the EU Hybrid Fusion Cell.

project[215]. Early July 2017, the new Estonian Presidency of the Council of the European Union asked the FoP to build, by the end of 2017, a "generic survey" that will enable the Member States "to better identify key indicators of hybrid threats, incorporate these into early warning and existing risk assessment mechanisms and share them"[216]. To that end, the Member States received a questionnaire about their individual knowledge of hybrid threats and relevant resilience capacity. They were encouraged to complete it – and provide, where possible, complementary information – by the end of September 2017. A summary of the answers will then be prepared in order to build the aforesaid "generic survey" and take further actions with a view to better countering "hybrid threats", for which field there is currently no centralised Belgian policy[217]. Moreover, this terminology can be confusing, in particular for non-militaries[218].

In order to enhance knowledge about "hybrid threats" and promote the exchange of information on this subject, the EU encourages the establishment of centres of excellence.

The EU "Hybrid Fusion Cell" and the NATO "Hybrid Analysis Branch"

The first initiative in this field dates back to May 2016 with the creation of an "EU Hybrid Fusion Cell" in Brussels within the EU Intelligence and Situation Centre (EU INTCEN) of the European External Action Service (EEAS). The main reason for its creation is the Ukrainian crisis. Consisting of seven people since June 2017, this Fusion Cell receives, analyses and shares "classified and open source information specifically relating to indicators and warnings concerning hybrid threats from different stakeholders within the EEAS (including EU Delegations), the Commission (with EU agencies), and Member States"[219]. A leading figure from EU INTCEN nevertheless highlights that, "contrary to the Cold War, when states controlled critical information, from now on [sometimes also] private companies control it [and this does not facilitate the exchange of data related to hybridity]"[220]. 21 EU Member States, including Belgium[221], have provided so far this Fusion Cell with National Contact Points "to ensure cooperation and secure communication"[222] with it. The Fusion Cell receives intelligence related to those threats on a voluntary basis. It monitors, inter alia, Russia and the "hybrid tools" used by this country, i.e. cyber technology and

---

[215] European Council, Presidency Note, *Mandate of the Friends of the Presidency Group on the Implementation of Action 1 of the Joint Framework on Countering Hybrid Threats (doc. 7688/16)*, 2 June 2017 [9502/17], p. 3.

[216] European Commission, Joint Report to the European Parliament and the Council on the implementation of the "Joint Framework on countering hybrid threats: a European Union response", Brussels, 19 July 2017, [JOIN (2017) 30 final], p. 4 (see annex 2).

[217] K. Haegens, *"Hybrid Warfare". Een onderzoek naar de Belgische militaire capaciteiten om deze vorm van oorlogvoering te bestrijden*, Belgian Royal Military Academy, Brussels, 28 April 2017, pp. 36 and 39; Statements collected in 2016 and 2017 by Captain-commandant (OF3) E. Hoorickx from Belgian civil servants in security-related ministries. They preferred to remain anonymous.

[218] Statements collected in 2016 and 2017 by Captain-commandant (OF3) E. Hoorickx from various military or non-military stakeholders holding key positions in security-related Belgian federal institutions.

[219] European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", 6 April 2016 [JOIN (2016) 18 final], p. 4.

[220] Interview at the EU INTCEN by Captain-commandant (OF3) E. Hoorickx, 30 November 2016.

[221] In January 2017, Belgium provided the name of two contact persons for the EU Hybrid Fusion Cell. Those persons respectively work in the Governmental Crisis and Coordination Centre (CGCCR) and in the Permanent Representation of Belgium to the EU.

[222] European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", 6 April 2016 [JOIN (2016) 18 final], p. 5.

propaganda. However, for lack of sufficient budgetary means, the Fusion Cell does not cover all hybrid threats developed by other countries. It does not address terrorist issues, which are the responsibility of the counter-terrorism department in the EEAS' Directorate for Conflict Prevention and Security Policy[223]. Since January 2017, it has released a periodical, *Hybrid Bulletin* analysing current hybrid threats. This document is shared within the EU institutions and bodies, as well as the national points of contact[224].

Until spring 2017, NATO did not have an organisation equivalent to the above-mentioned directorate in terms of analysis and exchange of information on "hybrid threats". The Atlantic Alliance could nevertheless already rely on a great number of centres of excellence dealing with issues linked to hybrid warfare, such as cyber defence or disinformation[225]. Furthermore, it has just implemented a Hybrid Analysis Branch, equivalent to the EU Hybrid Fusion Cell. This new NATO structure should facilitate the exchange of information between both institutions[226].

The European Centre of Excellence for Countering Hybrid Threats in Helsinki

Moreover, and in accordance with one recommendation specified in the April 2016 Joint Communication, a "European Centre of Excellence for countering hybrid threats" (Hybrid CoE) has been inaugurated in Helsinki on 11 April 2017. This Finnish "multinational and multidisciplinary"-oriented[227] project aims to improve knowledge on hybrid threats in order to better counter them[228]. The Centre is to work in close cooperation with both governmental and non-governmental experts, but also with the EU and NATO centres of excellence. Its first research projects will be launched in autumn 2017 and includes the preparation of a book on hybrid threats.

---

[223] Interview at the EU INTCEN by Captain-commandant (OF3) E. Hoorickx, 30 November 2016.

[224] European Commission, Joint Report to the European Parliament and the Council on the implementation of the "Joint Framework on countering hybrid threats: a European Union response", Brussels, 19 July 2017, [JOIN (2017) 30 final], p. 5.

[225] Since 2007, NATO has had a Joint Chemical, Biological, Radiological and Nuclear Defence Centre of Excellence in the Czech Republic (Vyškov); since 2008, a Cooperative Cyber Defence Centre of Excellence in Estonia (Tallinn); since 2012, an Energy Security Centre of Excellence in Lithuania (Vilnius) and, since 2015, a Strategic Communications Centre of Excellence (STRATCOM) in Lettonia (Riga) responsible for enhancing information security and protecting the allies' public space against disinformation (https://www.nato.int/cps/en/natohq/topics_68372.htm#). As for the EU, it has had an Institute for Security Studies since 2002 and thematic EU centres of excellence on CBRN issues since 2010 (European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", 6 April 2016 [JOIN (2016) 18 final], p. 6; R. Trapp, "The EU's CBRN Centres of Excellence Initiative after Six Years", in *Non-proliferation Papers*, February 2017, p. 1 [https://www.sipri.org/publications/2017/eu-non-proliferation-papers/eus-cbrn-centres-excellence-initiative-after-six-years]).

[226] S.n., *Progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016*, 14 June 2017, p. 3 (https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_06/20170619_170614-Joint-progress-report-EU-NATO-EN.pdf); European Commission, Joint Report to the European Parliament and the Council on the implementation of the "Joint Framework on countering hybrid threats: a European Union response", Brussels, 19 July 2017, [JOIN (2017) 30 final], p. 5.

[227] N. Gros-Verheyde, "Le premier centre d'excellence européen, sur les menaces hybrides, ouvre ses portes à Helsinki", in *bruxelles2.eu*, 19 April 2017.

[228] S.n., *EU Welcomes Establishment of the Finnish Centre of Excellence for Countering Hybrid Threats*, Brussels, 11 April 2017 (https://eeas.europa.eu/headquarters/headquarters-homepage/24572/eu-welcomes-establishment-finnish-centre-excellence-countering-hybrid-threats_en).

In addition, the Centre considers not only developing a doctrine, but also offering trainings and organising exercises "aiming at improving the participants' individual capabilities, as well as the interoperability between them, the EU and NATO in order to counter hybrid threats"[229]. Although the EU is not a signatory to the Memorandum of Understanding establishing the Centre, Federica Mogherini offered her "total support" to Finland for its creation[230]. She also encourages a "close working relationship" between the Centre and the EU Hybrid Fusion Cell[231].

By the end of 2017, this research centre in Helsinki employed ten full-time staff members who are part of a network with experts from all states participating in the project. Nine countries have signed the Memorandum of Understanding establishing the Centre by now: the United States, France, Great Britain, Poland, Finland, Sweden, Latvia, Lithuania, Norway and Spain[232]. Contrary to the EU Hybrid Fusion Cell, some Hybrid CoE member states are neither members of the EU nor NATO. However, as mentioned by B. Tigner, a senior NATO official states that "NATO often gets more information from its partner countries than its own allies"[233]. Moreover, according to a CI policy expert, "national governments don't want to reveal their vulnerabilities to each other"[234]. Hence the creation of the Centre of Excellence in Helsinki makes it possible to widen the reflection within NATO, where the hybrid warfare issue is the subject of discussions. Indeed, whereas it is largely associated with actions by Russia and the "Islamic State", NATO Member States' priorities often differ. Actually, according to R. Huygelen, Belgian Ambassador to NATO from 2010 to 2014, the Baltic States, Poland, Romania, or the Czech Republic want to remain able to face up to the Russian threat, whereas Southern Europe countries are geographically more concerned about conflicts in Africa or the fight against the "Islamic State"[235].

Before creating their Centre of Excellence, the Finns drew their inspiration from the Swedish concept of "total defence"[236], reactivated in December 2015 by Sweden in order to deal with the Russian danger. Finns and Swedes are, according to a leading figure from EU INTCEN, the "European Ivy League in fighting against hybrid threats"[237], particularly in the field of cyber security. During the official opening of the Centre of Excellence in Helsinki, Timo Soini, Finnish Minister for Foreign Affairs, highlighted that "[h]ybrid threats and hybrid tactics have become one of the most prominent security challenges […] in Europe[, and particularly in Finland]. Finland,

---

[229] N. Gros-Verheyde, *op. cit.*

[230] N. Gros-Verheyde, *op. cit.*; *Speech by Minister Soini at the Signing of the Memorandum of Understanding Establishing the European Centre of Excellence for Countering Hybrid Threats*, 11 April 2017 (https://um.fi/speeches/-/asset_publisher/up7ecZeXFRAS/content/ulkoministeri-soinin-puhe-hybridiosaamiskeskuksen-perustamistilaisuudessa?curAsset=0&stId=47307).

[231] N. Gros-Verheyde, "Le premier centre d'excellence européen, sur les menaces hybrides, ouvre ses portes à Helsinki", in *bruxelles2.eu*, 19 April 2017.

[232] *Ibid.*; S.n, "Helsinki: un lieu contre les 'menaces hybrides'", in *Le Figaro*, 11 April 2017 (http://www.lefigaro.fr/flash-actu/2017/04/11/97001-20170411FILWWW00212-helsinki-un-centre-contre-les-menaces-hybrides.php).

[233] B. Tigner, "An Evolving Threat", in *Jane's Defence Weekly*, 24 May 2017, p. 26.

[234] *Ibid.*, p. 29.

[235] Interview with R. Huygelen by Captain-commandant (OF3) E. Hoorickx, 16 July 2015.

[236] During the Cold War, Sweden, though officially neutral, conceived a vast "total defence" emergency plan involving civilians and the military, in case of a major incident with the USSR [S.n., "Suède : le retour de la 'défense totale'", in *Lettre d'informations stratégiques et de défense online* (www.ttu.fr), 28 July 2016; *Suède : les municipalités doivent se préparer à la guerre à la demande du gouvernement* (www.rt.com), 14 December 2016].

[237] Interview at the EU INTCEN by Captain-commandant (OF3) E. Hoorickx, 30 November 2016.

too, is a target for hybrid influencing[, f]or example, […] in the cyber domain"[238]. He also insisted on the use of hybrid elements in the recent crises: "During the ongoing migration crisis, we have seen elements of hybrid influencing by both state actors and non-state actors *[sic]*. Steering migration flows can be used as a method in political pressuring; and perpetrators of hybrid acts try to radicalise vulnerable members of society as their proxy actors"[239].

We need to examine a key concept of the fight against hybrid threats, i.e. "resilience", or the capability to resist and emerge stronger from "hybrid campaigns"[240]. In recent years, this word has become very fashionable within international circles. In 2012, it was the subject of a European Commission Communication on famine issues which were then affecting the Sahel and the Horn of Africa[241]. Even if this notion did not appear in the 2003 European Strategy nor in the report improving its implementation in 2008, it appeared in an EU strategic note in 2013 and was mentioned on almost every page of the second EU strategic document released in 2016[242]. On the other hand, this term does not appear in any NATO strategic concept, but was mentioned for the first time in the text of the 2014 Wales Summit Declaration[243]. Since then, the word "resilience" has regularly appeared in the documents relating to "hybrid threats"[244].

"Resilience" against "hybrid warfare practices"

The EU and NATO are committed to helping their member states to improve their "resilience", as well as their own resilience, against non-specifically military "hybrid warfare practices", i.e. sabotage, cyber attacks, propaganda, disinformation or CBRN attacks. In order to efficiently counter these practices, both organisations recommend their member states to protect

---

[238] N. Gros-Verheyde, "Le premier centre d'excellence européen, sur les menaces hybrides, ouvre ses portes à Helsinki", in *bruxelles2.eu*, 19 April 2017.

[239] *Ibid.*

[240] European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", 6 April 2016 [JOIN (2016) 18 final], p. 6.

[241] European Commission, Communication from the Commission to the European Parliament and the Council. The EU Approach to Resilience: Learning from Food Security Crises, 3 October 2012 [COM (2012) 586 final] (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0586).

[242] Note from the high representative of the European Union, A secure Europe in a better world – European security strategy, Brussels, 12 December 2003; European Council, Report on the Implementation of the European Security Strategy – Providing Security in a Changing World, Brussels, 11 December 2008 [S407/08] (https://europa.eu/globalstrategy/fr/node/12); European Commission, Joint Communication to the European Parliament and the Council: "The EU's comprehensive approach to external conflict and crises", 11 December 2013 [JOIN (2013) 30 final]; Note from the General Secretariat of the Council, "A Global Strategy for the European Union's Foreign and Security Policy", 28 June 2016 [EU's comprehensive approach, December 2013 CFSP 543, CSDP 395], p. 3, 6-7, 11, 16, 18, 19, 20-22, 27, 29, 37, 39 and 41 (https://ec.europa.eu/europeaid/sites/devco/files/a_global_strategy_for_the_european_unions_foreign_and_security_policy-_june_2016.pdf).

[243] NATO Press Release, *Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*, 5 September 2014, § 72-73.

[244] During the round-table discussion organised on 16 November 2016 in Brussels by the European Parliament ("*NATO-EU Cooperation after de Warsaw Summit: Countering Hybrid Warfare*"), all EU and NATO leading figures participating in the debate talked about "resilience". This conference gathered various experts, policy-makers, civil servants and industry representatives, in order to consider the content of the NATO Warsaw Summit and the EU and NATO projects in terms of countering hybrid threats.

their "potential vulnerabilities". The EU and NATO identify a large number of potential "weaknesses", i.e. protection of critical infrastructure (transports, (nuclear) power plants and space facilities), preparation to CBRN incidents or attacks, cyber defence, fight against terrorism or possibility to implement an efficient "strategic communication"[245]. It involves, should an enemy "systematically spread disinformation", the ability to "[p]rovid[e] factual responses and [to raise] public awareness about hybrid threats"[246]. This strategic communication should be consistent and effective before and during a hybrid conflict. Since 2015 the EU has had two task forces to help itself to manage this issue: "East StratCom" for issues related to Russia and "Arab StratCom" for issues related to the Middle East[247]. As for NATO, it has been assisted by its Strategic Communications Centre of Excellence in Riga since 2015. In July 2017, the EU also announced "[t]he upcoming launch of a new website: '#EUvsdisinformation' with an online search facility [that] will significantly improve user access"[248] and make it possible to warn against disinformation campaigns.

Belgium is attentive to improving its own "resilience", even if it is not part of a specific project to counter "hybrid threats". However, in its last Government Agreement, the Belgian Prime Minister recommended a "coordinated security approach", where the political level and public services need to collaborate efficiently, in particular in the fight against radicalisation, terrorism and cyber attacks[249]. Several Belgian royal decrees have indeed been signed so far in order to enhance the protection of Belgium's critical infrastructures. For instance, a new royal decree was signed in February 2016 in order to improve the security and protection of critical infrastructures in the rail transport[250]. In May 2017, the European Commission organised a workshop on hybrid threats against critical infrastructures which was attended by almost every Member State, as well as critical infrastructures managers, the EU Hybrid Fusion Cell and NATO, as an observer. The Commission will once more consult the stakeholders in autumn, in order to adopt indicators designed to improve the protection and resilience of critical infrastructures against hybrid threats before the end of 2017[251]. Furthermore, Belgium benefits from a cyber security strategy aiming, inter alia, at "the optimum protection and securing of critical infrastructures and public systems against cyber threat"[252]. The "Belgian Cyber Security Centre" nevertheless highlighted

---

[245] European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", 6 April 2016 [JOIN (2016) 18 final], pp. 6-18.

[246] *Ibid.*, p. 5.

[247] *Ibid.*

[248] European Commission, Joint Report to the European Parliament and the Council on the implementation of the "Joint Framework on countering hybrid threats: a European Union response", Brussels, 19 July 2017, [JOIN (2017) 30 final], p. 5.

[249] *Accord de gouvernement* (Belgian Government Agreement), 9 October 2014, pp. 131, 143 and 147 (http://www.premier.be/fr/accord-de-gouvernement).

[250] *Arrêté royal du 19 février 2016 relatif à la sécurité et la protection des infrastructures critiques, pour le secteur du Transport, sous-secteur du transport ferroviaire* (Belgian Royal Decree of 16 February 2016 on Security and Protection of Critical Infrastructures, for the Transport Sector, Subsector Rail Transport), in *Moniteur belge*, 7 April 2016, pp. 23017-23023.

[251] European Commission, Joint Report to the European Parliament and the Council on the implementation of the "Joint Framework on countering hybrid threats: a European Union response", Brussels, 19 July 2017, [JOIN (2017) 30 final], p. 7.

[252] European Union Agency for Network and Information Security, *Belgian National Cyber Security Strategy*, 23 November 2012, p. 7 (https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/belgian-cyber-security-strategy/view).

shortcomings in terms of "nuclear cyber security"[253]. The Member States are bound to implement the EU "directive on nuclear safety"[254] into their own legislation by the end of 2017. The public limited company Engie-Electrabel also wrote its own "nuclear security plan for 2016-2020"[255]. The Belgian Federal Police's "national security plan for 2016-2019" also highlights the importance of countering terrorism, violent extremism, organised crime and "cybercrime"[256]. The Belgian Government also makes the fight against "Daesh" one of its priorities. This fight materialises in various fields, such as improving cooperation between the ministries of Home Affairs and Justice, tracking the terrorist network financing, protecting the population and infrastructures, through the help of the Belgian Defence but also by developing a deradicalisation programme[257]. Moreover, on demand of the European Commission, all Member States were compelled to implement the EU's Fourth Anti-Money Laundering Directive at the end of June 2017 in order to combat terrorist financing[258].

In January 2017, ACOS Ops & Trg developed a "strategic communication" doctrine highlighting the importance of proactivity rather than reactivity to disinformation[259]. There exists within the Belgian Defence a genuine desire to extend this project to other Belgian political instances in order to implement a national policy in this field[260]. Some people indeed regret that there is no real strategy against Russian disinformation campaigns[261]. When in October 2016 Moscow accused Belgium of having participated in bombings responsible for the death of civilians around Aleppo, the Ministry of Foreign Affairs categorically denied the facts, "deeply regretting the absence of previous consultation aiming to establish the facts, before these accusations were rendered public"[262]. According to some, this incident had something of "a smoke screen in a moment when the international community [considered] sanctions against the Syrians and the Russians for the heavy and undiscriminating bombings of rebel positions in Aleppo"[263].

---

[253] Document parlementaire de la Chambre des représentants belge (Rapport d'audition), *La cybersécurité des centrales nucléaires en Belgique*, (Belgian Chamber of Representatives Parliamentary Document, Audition Report, Nuclear Power Plant Cybersecurity in Belgium), 20 January 2017, p. 6 (http://www.lachambre.be/FLWB/PDF/54/2274/54K2274001.pdf).

[254] European Commission, Joint Report to the European Parliament and the Council on the implementation of the "Joint Framework on countering hybrid threats: a European Union response", Brussels, 19 July 2017, [JOIN (2017) 30 final], p. 8.

[255] Ph. Van Troeye, *Plan de sûreté nucléaire 2016-2020 d'Electrabel*, s.d. (https://culturesurete.be/data/16011_gp_nucleaire_veiligheid_fr_lr1.pdf).

[256] G. Bomal (under the direction of), *Plan national de sécurité de la police fédérale 2016-2019*, s.d.

[257] D. Leroy, "La Belgique et Daesh : état des lieux", in *Revue militaire belge*, No 14, July 2017, p. 67.

[258] European Commission, Joint Report to the European Parliament and the Council on the implementation of the "Joint Framework on countering hybrid threats: a European Union response", Brussels, 19 July 2017, [JOIN (2017) 30 final], p. 14.

[259] Belgian Ministry of Defence, *Strategic Communications*, ACOT-COD-STRATCOM-DCOJ-001-DRC2/DRC2, Ed 001/Rev 000.

[260] K. Haegens, *"Hybrid Warfare". Een onderzoek naar de Belgische militaire capaciteiten om deze vorm van oorlogvoering te bestrijden*, Belgian Royal Military Academy, Brussels, 28 April 2017, p. 37.

[261] *Ibid.*

[262] S.n., "Bombardement en Syrie : la Russie accuse toujours la Belgique, mais les numéros d'avions ne correspondent pas", (www.rtbf.be), 20 October 2016.

[263] *Ibid.*

Although the EU and NATO show good intentions in terms of "resilience" and are resolute to use the existing "policies and instruments"[264], it seems that, so far, cyber security benefits from the most substantial follow-up. Accordingly, the EU directive on security of network and information systems (NIS directive), adopted on 6 July 2016, specifies new cyber security obligations for the Member States and some companies in order to create a reliable cyber environment within the EU[265]. It is planned that, by May 2018, Belgium reviews its cyber strategy in the light of this directive. This mission will be monitored by the "Belgian Cyber Security Centre"[266]. Cyber security is a priority for the Belgian government, in particular in order to "ensure an optimum securing and protection of critical infrastructures"[267]. Since 2009, Belgium also has an "emergency intervention team in IT security" – named "CERT" (Computer Emergency Response Team[268]) – which is allowed, in case of IT emergency, to cooperate with CERT-EU, the EU's interinstitutional computer emergency response team[269]. It should finally be noted that a European Centre for Cybersecurity in Aviation, also cooperating with the CERT-EU, was established in February 2017[270].

The "cyber defence" issue is also at the centre of NATO attention. Indeed, since 2008, the Atlantic Alliance has had a centre of excellence for cyber defence in Tallinn, Estonia. Not only does it conduct exercises, but also research and training activities in technical, legal and strategic fields related to cyber security[271]. Since January 2017, Belgium has also participated in activities within the Centre, alongside with sixteen other Atlantic Alliance countries[272]. During the Warsaw Summit in July 2016, the Atlantic Alliance also "recognise[d] cyberspace as a domain of operations in which

---

[264] European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", 6 April 2016 [JOIN (2016) 18 final], p. 3.

[265] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, in *Official Journal of the European Union*, 19 July 2016 (https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG).

[266] A. Dammekens, *Cybersécurité – la directive européenne impose aux entreprises l'obligation de notifier les cyberincidents*, 12 July 2016 (http://www.vbo-feb.be/fr-BE/domaines-daction/securite--bien-etre-au-travail/securite-des-entreprises/cybersecurite--la-directive-europeenne-impose-aux-entreprises-lobligation-de-notifier-les-cyberincidents_2016-07-12/). The "Belgian Cyber Security Centre", created in October 2014 and coming under the authority of the Prime Minister, is in charge of preparing a cyber security strategy for Belgium, ensuring crisis management in case of cyber incidents, in cooperation with the government's Coordination and Crisis Centre, give opinions on the policy to be pursued and take initiatives in order to advise and protect companies, consumers and public authorities (*Accord de gouvernement*, 9 October 2014, p. 148; http://www.ccb.belgium.be).

[267] *Accord de gouvernement* (Belgian Government Agreement), 9 October 2014, p. 148.

[268] The Belgian "CERT" depends on the Belgian Cyber Security Centre and has a double mission: on the one hand, coordinating the management and response to nationwide incidents with operators of critical infrastructures and essential services as well as, on the other hand, serving as information hub in terms of cyber security (http://www.ccb.belgium.be).

[269] The CERT-EU, operational since September 2012, ensures the European institutions' cyber security and cooperates with other CERTs in the Member States (https://cert.europa.eu/cert/plainedition/en/cert_about.html).

[270] European Commission, Joint Report to the European Parliament and the Council on the implementation of the "Joint Framework on countering hybrid threats: a European Union response", Brussels, 19 July 2017, [JOIN (2017) 30 final], p. 9.

[271] https://ccdcoe.org/about-us.html.

[272] S.n., "La Belgique a rejoint le centre d'excellence de l'Otan pour la défense cybernétique" (www.rtbf.be), 26 April 2016.

NATO must defend itself as effectively as it does in the air, on land, and at sea"[273]. Hence it "committed to enhance the cyber defences of [its] national networks and infrastructures, as a matter of priority"[274]. In early December 2016, the EU and NATO approved a number of cooperation measures in terms of cyber security, related to exchange of information, training and participation in common exercises[275]. In February 2017, the NATO Defence Ministers approved an "updated Cyber Defence Action Plan" as well as a "roadmap to implement cyberspace as a domain of operations" in order to "increase Allies' ability to work together, develop capabilities and share information". Finally, the EU and NATO have started to incorporate cyber attacks in their annual "crisis management" exercises, which from now on take place in a fictive hybrid threat environment. The first training involving both organisations in a hybrid attack scenario will take place in September-October 2017. During this exercise, called "PACE17" (Parallel and Coordinated Exercise), the enemy will not only resort to "cyber attacks" against its adversary's critical infrastructures, but also to propaganda[276]. "Strategic communication" also plays an important part in those individual exercises in which Belgium participates.

Preventing and responding to hybrid threats effectively

The effectiveness of prevention and response in case of hybrid attack is the fifth element of the strategy proposed by the EU and NATO. When the author of a hybrid attack is revealed, both organisations aim at fighting the threat. However, because of their very essence and their capabilities, the reaction of each organisation will be different.

NATO strategy

NATO's determination to be ready to respond swiftly and firmly to new security challenges from the east and the south is in line with the "Readiness Action Plan" (RAP) launched by NATO during its Wales Summit in 2014 and reaffirmed at the Warsaw Summit in 2016. This plan is the most significant reinforcement of NATO's collective defence since the end of the Cold War[277]. In case of a hybrid attack on an allied country, the NATO Council could invoke Article 5 of the Washington Treaty, as it would in case of an armed attack[278].

Belgium has taken part in both components of the "Readiness Action Plan" since 2016. It contributes, on the one hand, to this project's "assurance measures", aimed at reassuring the

---

[273] NATO Press Release, *Warsaw Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016*, § 70.

[274] *Ibid.*, § 71.

[275] European Parliament, *Countering hybrid threats: EU-NATO cooperation*, March 2017 (http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf).

[276] European Commission, Joint Report to the European Parliament and the Council on the implementation of the "Joint Framework on countering hybrid threats: a European Union response", Brussels, 19 July 2017 [JOIN (2017) 30 final], pp. 18-19.

[277] S.n., *Readiness Action Plan*, 1 March 2017 (https://www.nato.int/cps/uk/natohq/topics_119353.htm?selectedLocale=en).

[278] S.n., "Les attaques hybrides provoqueront une réponse militaire collective de l'OTAN" (www.rt.com), 1 December 2015.

populations of Central and Eastern European countries through reinforcing their defence[279]. In this context, the Belgian armed forces participate in the "Enhanced Air Policing Mission" and to demining operations in the Baltic Sea[280]. On the other hand, it contributes to the RAP "adaptation measures" that will allow the Alliance to be better able to "react swiftly and decisively to sudden crises"[281]. For this reason, the Belgian armed forces make troops and means from their three components available to the new "Very High Readiness Joint Task Force" (VJTF) that will be able to deploy within a few days to "respond to challenges that arise, particularly at the periphery of NATO's territory"[282].

An "implementation plan" for the NATO strategy on countering hybrid warfare was prepared in February 2016. Its aim is to improve NATO's capability to countering hybrid warfare practices, but also the Alliance member countries' resilience. Some countries reaffirmed their determination to commit militarily in the fight against hybrid threats. For instance, the Dutch minister of Defence released a note where he highlighted the important role that armed forces can play in order to "anticipate", but also to counter hybrid campaigns. They not only represent important "deterrence", but also "protection" means for vital infrastructures[283]. In his most recent "*Strategic Vision for Defence*" issued in June 2016, the Belgian minister of Defence also acknowledged the importance of the "hybrid warfare" issue, defined as a warfare that "combines military and non-military means and methods to destabilise countries"[284]. Besides, he was aware that "[e]ffective intelligence services are an essential first link in quickly identifying and understanding hybrid threats, in order to respond rapidly and avoid escalation [...]"[285] and that "[a]verting hybrid threats also requires a reinforcement of the comprehensive approach and therefore the use of all power elements to support stability and security"[286]. He finally underlined the importance for our military cyber capability to be reinforced in order to meet the needs of collective defence[287].

It is noteworthy that, since 2015, the Lithuanian National Defence Ministry has been distributing to the Lithuanian citizens an explanatory and advisory guide in case of attacks or emergency situations. This document explains, for example, how to face a CBRN attack or how to recognise "little green men"[288]… Some indeed consider that the Baltic States fear the Ukrainian scenario to be exported to their own countries. Those former USSR republics indeed have significant Russian minorities and fear the emergence of separatist movements supported by

---

[279] S.n., *Readiness Action Plan*, 1 March 2017 (https://www.nato.int/cps/uk/natohq/topics_119353.htm?selectedLocale=en).

[280] S. Vandeput, *Communiqué de presse du 2 décembre 2016 sur les opérations 2017* (press release on the operations in 2017, 2 December 2016) (http://www.vandeput.belgium.be/fr/op%C3%A9rations-2017).

[281] S.n., *Readiness Action Plan*, 1 March 2017 (https://www.nato.int/cps/uk/natohq/topics_119353.htm?selectedLocale=en).

[282] NATO Press Release, *Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*, 5 September 2014, § 8.

[283] K. Haegens, *"Hybrid Warfare". Een onderzoek naar de Belgische militaire capaciteiten om deze vorm van oorlogvoering te bestrijden*, Belgian Royal Military Academy, Brussels, 28 April 2017, p. 35.

[284] Belgian Ministry of Defence, *The strategic vision for Defence*, Brussels, 29 June 2016, p. 28.

[285] *Ibid.*, p. 41.

[286] *Ibid.*, p. 42.

[287] *Ibid.*, p. 53.

[288] Lithuanian National Defence Ministry, *Prepare to Survive Emergencies and War: a Cheerful Take on Serious Recommendations*, Vilnius, 2015.

Moscow[289]. It is also noteworthy that, between 2009 and 2016, from all NATO countries, not only Romania and Poland, but also the Baltic States have increased the GDP percentage attributed to defence expenditure[290]. This percentage is close to 1.5%, and even exceeds, for Estonia and Poland, the NATO 2% requirement[291].

EU strategy

In order to be better prepared to react swiftly "to events triggered by hybrid threats"[292], the EU High Representative recommends three specific actions. First of all, it is necessary to consider the applicability and practical implications of EU's legal prescriptions to cope with "hybrid threats". The Permanent Representative reminds that "if multiple serious hybrid threats constitute armed aggression[293] against an EU Member State, [the mutual assistance clause of] Article 42 (7) TEU [Treaty on European Union][294] could be invoked to provide an appropriate and timely response"[295]. Indeed, "[g]iven the ambiguity associated with hybrid activities, the possible last resort applicability of the Solidarity Clause [which is described in Article 222 TFEU (Treaty on the Functioning of the European Union) and relates to terrorist attacks and natural or man-made disaster an EU country could be the victim of[296]] should be assessed by the Commission and the High Representative (in

[289] S.n., "La menace russe pèse sur les pays baltes", in *La Croix* (https://www.la-croix.com/Actualite/Europe/La-menace-russe-pese-sur-les-pays-Baltes-2015-03-03-1286767), 3 March 2015.

[290] According to NATO terminology, the concept of "defence expenditure" includes all payments for defence in every sense. As for Belgium, "defence expenditure" covers the national Defence budget as well as the military and civilian pensions of the Defence personnel depending on the Belgian Federal Pensions Service (Ph. Manigart, *L'évolution des dépenses militaires en Belgique depuis 1900*, CHCRISP No 1009, Brussels, 30 September 1983, p. 4; Belgian Ministry of Defence, *The strategic vision for Defence*, 29 June 2016, p. 74).

[291] *Defence Expenditure of NATO Countries (2009-2016)*, 13 March 2017, p. 2 [communiqué PR/CP(2017)045] (https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_03/20170313_170313-pr2017-045.pdf)

[292] European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", 6 April 2016 [JOIN (2016) 18 final], p. 18.

[293] United Nations Resolution 3314 of 14 December 1974 defines an "aggression" as "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations [...]" (Article 1 of United Nations General Assembly Resolution 3314 of 14 December 1974) (http://www.un-documents.net/a29r3314.htm).

[294] Article 42(7) of the Treaty on European Union reads as follows: "If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter. This shall not prejudice the specific character of the security and defence policy of certain Member States. Commitments and cooperation in this area shall be consistent with commitments under the North Atlantic Treaty Organisation, which, for those States which are members of it, remains the foundation of their collective defence and the forum for its implementation" (the Treaty on European Union (consolidated version) is available on https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF).

[295] European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", 6 April 2016 [JOIN (2016) 18 final], p. 19.

[296] Article 222 of the Treaty on the Functioning of the European Union reads as follows: "The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States, to [...] assist a Member State in its territory, at the request of its political authorities, in the event of a terrorist attack [...]" (the Treaty on the Functioning of the European Union (consolidated version) is available on https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=CELEX:12012E/TXT&from=en). The EU defines terrorist offences as "intentional acts [...] which, given their nature or context, may seriously damage a country or an international organisation where committed with the aim of seriously intimidating a population, or unduly compelling a Government or

their respective areas of competence), in case an EU Member State is subject to significant hybrid threats"[297].

For instance, after the terrorist attacks in Paris in November 2015, the president of the French Republic preferred to invoke Article 42(7) TEU rather than Article 222 TFEU, though the latter seemed precisely written for that kind of tragic occasion. Although the mutual assistance clause of Article 42(7) TEU might not totally match with the situation, for example because of age-long debates dividing the international community on the notion of "armed aggression", the French choice can be explained by various political and legal reasons[298]. One of the significant reasons for this choice is that Article 222 TFEU only concerns an international assistance on the territory of Member States, what France did not want[299]. On the contrary, when invoking the Article 42(7) TEU clause rather than Article 222 TFEU, or even Article 5 of NATO Treaty enshrining the collective defence principle, France could preserve the control of its sovereignty, including its foreign policy, while seeking to strengthen the Europeans' involvement in international counter-terrorist operations in order to lighten the French military presence[300].

Afterwards, with a view to reacting swiftly and efficiently in case of a hybrid attack, a common operational protocol established by the Commission between itself, the Member States and the High Representative specified in July 2016 the role of each Union institution and actor in the procedures to be applied in case of a hybrid campaign, from the initial identification phase to the final phase of attack[301]. This document will be tested in autumn 2017 as part of the EU Parallel and Coordinated Exercise in 2017 (PACE17) under NATO command, in which the EU will participate[302]. This exercise will test the EU's various mechanisms and ability to interact "with the goal of speeding decision making where ambiguity triggered by a hybrid threat detracts from clarity"[303].

In the end, the High Representative encourages Member States to examine the military action capabilities to be implemented in countering hybrid threats, in the context of the Common

---

international organisation to perform or abstain from performing any act, or seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation [...]" (Article 1 of the *Council Framework Decision of 13 June 2002 on combating terrorism*, available on https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002F0475&from=EN).

[297] European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", 6 April 2016 [JOIN (2016) 18 final], p. 19.

[298] F. Gouttefarde, "L'invocation de l'article 42§7 TUE : la solidarité militaire européenne contre le terrorisme", in *RDN*, March 2016, pp. 68-69. According to F. Gouttefarde, terrorist acts cannot constitute crimes of aggression, because this latter type of crime presupposes the existence of two sovereign states recognised by the international community, one being the aggressor and the other the victim (*Ibid.*, p. 72).

[299] *Ibid.*, p. 73.

[300] F. Gouttefarde, "L'invocation de l'article 42§7 TUE : la solidarité militaire européenne contre le terrorisme", in *RDN*, March 2016, pp. 73 and 76.

[301] European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", 6 April 2016 [JOIN (2016) 18 final], p. 19 (see annex 1).

[302] European Commission, Joint Report to the European Parliament and the Council on the implementation of the "Joint Framework on countering hybrid threats: a European Union response", Brussels, 19 July 2017, [JOIN (2017) 30 final], p. 18.

[303] *Ibid.*, p. 19.

Security and Defence Policy (CSDP)[304]. In this context, the European Commission affirms that "capabilities priorities to strengthen resilience against hybrid threats identified by Member States might [...] be eligible for support under the European Defence Fund as of 2019"[305]. The European Defence Agency takes part, with various studies, in the reflection on the implementation of new military action capabilities aiming to counter hybrid threats. For instance, an analysis is scheduled for 2018 on the military role in the context of countering mini-drones, which are likely to be used against critical infrastructures[306]. Moreover, various meetings have been organised by the European Union military staff (EUMS), as well as by the Directors-General in charge of EU Defence Policy. Those discussions in which Belgium participated show that the military contribution related to "hybrid threats" will be relatively limited, will not need specific military capabilities to be implemented and will be conditional on the civilian-political approach in any event. "Hybrid threats" nevertheless affect military priorities, concepts and doctrines[307].

Moreover, according to the Member States' representatives who attended the meetings, the interdepartmental cooperation and the existing national structures should suffice to face "hybrid threats"[308]. Belgium indeed has various organs in charge of coordinating the national security policy, whatever the threat level. Those organs are the National Security Council, responsible for establishing and coordinating the national general intelligence and security policy[309]; the Governmental Crisis and Coordination Centre (CGCCR), which ensures a 24/24 collection and distribution of "any kind of urgent information" to the competent authorities[310]; and the Coordination Unit for Threat Assessment (CUTA), in charge of achieving strategic and temporary assessments on terrorist and extremist threats against Belgium[311]. Various "emergency plans" aiming to improve the coordination of the responsible authorities' actions exist in Belgium[312].

---

[304] European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", 6 April 2016 [JOIN (2016) 18 final], p. 19.

[305] European Commission, Joint Report to the European Parliament and the Council on the implementation of the "Joint Framework on countering hybrid threats: a European Union response", Brussels, 19 July 2017, [JOIN (2017) 30 final], p. 10.

[306] *Ibid*.

[307] "*Workshop on the EU Military Contribution to Countering Hybrid Threats. 13/14 Dec 2016, Lisbon*", unpublished document; *EU Defence Policy Directors Meeting*, Brussels, 5 May 2017, unpublished document.

[308] "*Workshop on the EU Military Contribution to Countering Hybrid Threats. 13/14 Dec 2016, Lisbon*", unpublished document; *EU Defence Policy Directors Meeting*, Brussels, 5 May 2017, unpublished document.

[309] Created in February 2015, the National Security Council establishes the general intelligence and security policy, ensures its coordination, and determines the priorities of the intelligence and security services. It is also in charge of coordinating the fight against terrorist financing and against the proliferation of weapons of mass destruction. It also defines the protection of sensitive information. The National Security Council is presided by the Prime Minister, and includes the ministers in charge of Justice, Defence, Home and Foreign Affairs, as well as the Vice-Prime Ministers who are not in charge of those fields (www.premier.be).

[310] Created in 1986, the Governmental Crisis and Coordination Centre (CGCCR) ensures an uninterrupted 24/7 duty for collecting, analysing and distributing "any kind of urgent information" to the competent authorities, including news about terrorism, cyber incidents, public health, rail accidents, natural disasters, and the nuclear field (www.centredecrise.be).

[311] Created in 2006, the Coordination Unit for Threat Assessment (CUTA) is in charge of achieving strategic and temporary assessments on terrorist and extremist threats against Belgium. Accordingly, it establishes the "threat scale" on the basis of information collected from several organs such as the Belgian State Security Service, the Belgian federal and local polices and various Belgian Federal Public Services (www.centredecrise.be).

[312] *Arrêté royal relatif aux plans d'urgence et d'intervention* (Royal decree on emergency and intervention plans), 16 February 2006; *Arrêté royal portant fixation du plan d'urgence national relatif à l'approche d'une prise*

The EU and NATO want to improve their member states' and their own respective capability to react to "hybrid campaigns". In order to do so, both organisations advocate strengthening their cooperation in this field.

EU-NATO cooperation

The EU and NATO intend to increase their cooperation in order to respond more efficiently to "hybrid threats". The EU manifested this determination as of May 2015 and NATO responded favourably to this offer some months later[313]. Indeed, "[t]he two organisations share values and face similar challenges"[314]. Therefore, they wish to develop a shared situational awareness of hybrid risks, implement consistent strategic communications before and during a hybrid conflict[315], but also collaborate in the field of cyber security as well as "crisis prevention and response"[316]. The High Representative however pointed out that any closer interaction between the EU and NATO must occur "while respecting each organisation's decision-making autonomy and data protection rules"[317].

According to an individual statement from an INTCEN official, the exchange of information related to hybrid threats between the EU and NATO is still not sufficient and should be improved. Indeed, the legal information transmission procedures are quite complicated, and "the functioning of NATO is a very procedural system, contrary to the EU which produces more consensual documents than NATO does, and works more fluidly"[318].

In its conclusions issued in December 2016, the Council of the European Union welcomed the Joint Declaration of July 2016, because it "gives new impetus and substance to EU-NATO cooperation in the areas of countering hybrid threats [...]"[319]. In July 2017, the European Commission assessed the Joint Communication of April 2016 entitled "Joint Framework on countering hybrid threats: a European Union response". The subsequent report demonstrated that

---

d'otage terroriste ou d'un attentat terroriste (Royal decree determining the national emergency plan on the approach to be adopted in case of hostage-taking or a terrorist attack), 1 May 2016.

[313] European Defence Agency, *Hybrid Warfare Threats – Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 November 2015 [SCS/P003198], pp. 21-22.

[314] European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", 6 April 2016 [JOIN (2016) 18 final], p. 20.

[315] European Defence Agency, *Hybrid Warfare Threats – Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 November 2015 [SCS/P003198], p. 22.

[316] European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", 6 April 2016 [JOIN (2016) 18 final], p. 20.

[317] *Ibid.*

[318] Interview at the EU INTCEN by Captain-commandant (OF3) E. Hoorickx, 30 November 2016.

[319] European Council, Council conclusions on the Implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization, 6 December 2016 [PESC 1004, PSDC 699, COPS 378, POLMIL 147, EUMC 146], p. 2 (http://data.consilium.europa.eu/doc/document/ST-15283-2016-INIT/en/pdf).

the EU and NATO joint efforts undertaken throughout 2017 "have delivered substantial results"[320]. Indeed, in addition to EU-NATO cooperation in the cyber defence research and technology field, this report mentioned the following developments: the interaction between the EU "Hybrid Fusion Cell" and the NATO "Hybrid Analysis Branch", the organisation in October 2017 of a first common EU-NATO exercise (PACE17) in order to test "their response to a hybrid scenario", as well as their common participation in mutual information sessions on resilience to hybrid threats. The next progress report on EU-NATO cooperation will suggest possibilities for expanding cooperation between the two organisations in this field[321].

[320] European Commission, Joint Report to the European Parliament and the Council on the implementation of the "Joint Framework on countering hybrid threats: a European Union response", Brussels, 19 July 2017, [JOIN (2017) 30 final], p. 20.

[321] *Ibid.*, pp. 19-20.

Conclusions and Recommendations[322]

Observations

Hybrid threats, conflicts and warfare

Whereas the use of hybrid methods is as old as warfare itself, the concept of "hybrid warfare" or "hybrid threats" only recently covers a vast semantic reality, where the adversary can just as well use conventional and non-conventional "hard power" as well as "soft power". According to some, the engagement of kinetic actions is not a *sine qua non* condition for hybrid strategy. This is actually what distinguishes "hybrid conflicts" from "hybrid warfare", which notion was used for the first time in the context of an armed conflict in order to term the Chechen insurgency.

In scientific circles, hybrid warfare practices are linked with very diverse actors. However, it is evident that Russia figures prominently in the debates about this issue. Some even consider that the Russian hybrid strategy is the "comprehensive approach gone over to the dark side of the force".

The concepts of "hybrid threats" and "hybrid warfare" – this latter term being preferred by NATO since 2014 – are terminologies evolving over time and according to the international situation. The first definitions provided by the Atlantic Alliance appeared in the context of the Russian interventions in former USSR socialist republics, i.e. Estonia, Georgia and Ukraine. Initially, the concept of "hybrid threats" covers the simultaneous use of conventional and non-conventional means. Later, when the Russian-Ukrainian crisis broke out, "hybrid warfare" indicated the – very integrated – implementation of military and non-military means in order to destabilise an adversary. The EU disclosed its first definition of "hybrid warfare" in May 2015, after the particularly bloody terrorist attacks in France. Although this definition is largely inspired from NATO's own definition, it contains more details on the operating modes of "hybrid warfare" or "ambiguous warfare", i.e. cyber attacks, disinformation, sabotage and "proxy warfare". "Hybrid attacks" aim to exploit the "vulnerabilities" of individual states and to prevent a coordinated response from the international community. Some months later, NATO developed its first strategy in order to counter "hybrid warfare practices", in which stakeholders can now be either "state actors" or "non-state actors". It is indeed presumed that the "Islamic State" also uses certain hybrid practices, though without having – as Russia does – sophisticated power structures, including an established diplomatic network. The complexity of hybrid warfare is such that only an individualised approach can make it possible to have a deep understanding of Russia and the Islamic State in that field. Moreover, it is still to be determined if Daesh' terrorist acts qualify as "warfare".

Within the EU, the term "hybrid threat(s)" is preferred to the term "hybrid warfare" used by NATO. This plurality of denominations can stir up some semantic confusion. Furthermore, the terminology used does not seem to have the same meaning amongst the EU civilian and military circles. For the EU Military Staff, the notion of "hybrid threat" describes the combined use of "hybrid warfare practices" and is therefore used as a synonym for "hybrid warfare". On the contrary, in the civilian circles, the concept of "hybrid threats" seems to be directly associated with various fields such as sabotage, cyber attacks, propaganda, disinformation, and CBRN attacks. A "hybrid threat" would in that case correspond to a specific operating mode, which is contradictory to the very meaning of "hybridity", which can by definition only designate a combination of two elements. Nevertheless – and this is what makes the issue even thornier – in order those "threats" to be considered as "hybrid",

[322] This study's conclusions will shortly be the subject of a paper entitled "Quelle stratégie euro-atlantique face aux « menaces hybrides » ?" (E. Hoorickx), in *Revue Défense Nationale (RDN)*.

they need to be combined with each other and used in order to achieve some precise political objectives. Moreover, the emergence of the concept of "resilience" contributes to making the notion even more complex. Indeed, when the EU recommends to its Member States to counter "hybrid threats", it actually encourages them to reduce their "potential vulnerabilities" in, for instance, the fight against terrorism or organised crime. It is a short step from this observation to associating "hybrid threats" with the states' "weaknesses". In any event, it is obvious that the notion of hybridity is not understood the same way by all parties.

Therefore, it is not surprising that the notion of "hybrid warfare" does not win unanimous support. Some question the usefulness of such a catch-all term – which is often associated with another cliché term: "resilience" – and even talk about a "*reinvention of the wheel*" for the sake of NATO bureaucracy. As far as strategy is concerned, this position makes sense. The overall strategy, proxy warfare and information warfare are indeed traditional practices from a historical perspective, even when those elements are integrated in the same operation. Moreover, the security challenges identified in NATO strategic documents as from 1991 and in EU strategic documents as from 2003 have covered all the "hybrid warfare practices" or "hybrid threats" mentioned in both organisations' official press releases since the early 2010s. Only the cyber security issue appeared more recently as a new strategic challenge, i.e. in 2010 within NATO and 2013 within the EU.

If there is something new, it has to be found on the tactical/operational side of "hybrid warfare". Cyber threat, the massification of fighters' "*de-identification*" during the Russian-Ukrainian crisis and the appropriation – by an irregular enemy like "Daesh" – of advanced technologies which became ergonomic, are convincing examples thereof.

Five elements for a strategic response

"Hybrid warfare" practices are considered a major security challenge by the EU and NATO, which in 2015 aimed to develop – each one separately but through cooperation – a consistent strategy in fighting against "hybrid campaigns", in order to help their respective member states to counter this complex threat. The strategic response proposed by the EU and NATO focuses on five elements: improving awareness about "hybrid practices", building resilience against them, efficiently preventing and responding to hybrid attack ("*Integrated Political Crisis Response*") and, finally, a better coordination between the parties in all these issues, including strategic communication and cyber security. Although both organisations commit to supporting their member states in countering "hybrid campaigns", they point out that the primary responsibility lies with these latter ones. They are also determined to draw on the existing "policies and instruments" in order to tackle this issue.

The EU and NATO take concrete measures in order to fight against "hybrid warfare practices". First of all, in order to better study them, the EU has, since May 2016, been in a position to resort to a cell in charge of centralising and sharing information linked to this issue. Since spring 2017, NATO has had its own equivalent cell, which should facilitate the exchange of information with the EU. Secondly, cyber defence is a priority in terms of "resilience". The EU made strict recommendations to its Member States so that they would define their cyber security strategy. Furthermore, NATO and the EU are beginning to incorporate the issue of "cyber attacks" in their common as well as separate exercises. The training scenarios have also recently included the vulnerability of critical infrastructures and propaganda.

Ultimately, in order to respond swiftly and decisively to a potential "hybrid campaign", the Atlantic Alliance can rely on the "Readiness Action Plan" (RAP) launched in 2014. As for the EU, it has had, since July 2016, an operational protocol between Member States, the European Commission and the High Representative, mapping the role of each Union institution and actor in the procedures to follow in case of hybrid campaign, from the initial identification phase to the final phase of attack. The applicability and practical implications of the EU and NATO legal provisions aimed to deal with

hybrid threats are the subject of major discussions. Moreover, in the case of the EU, the military contribution is relatively limited, does not need specific military capabilities to be implemented and is at any rate conditional on the political approach. "Hybrid threats" however have an impact on the military priorities, concepts and doctrines. On the national level, the interdepartmental cooperation and the existing national structures should also suffice to respond to "hybrid campaigns".

Belgium's policy for countering hybrid threats

Belgium invests a lot in its cyber security and equips itself with the necessary instruments to improve its resilience and respond to the EU and NATO recommendations in this field. Fighting radicalisation and terrorism as well as protecting critical infrastructures are also part of the Belgian State's security priorities. So far, Belgium has no centralised policy concerning the fight against "hybrid threats". It however has several bodies in charge of coordinating the national security policy, regardless of the level of the threat, whether "hybrid" or not. Moreover, Belgium's Ministry of Defence, which considers "hybrid warfare" as a challenge of the highest importance, actively participates in NATO's "Readiness Action Plan" (RAP).

Recommendations

Adopting a common terminology

If the EU and NATO consider it necessary to have a specific terminology in order to define attacks using military or non-military means in order to exploit other states' "vulnerabilities", preventing – in doing so – a coordinated response from them, it is urgent that they both speak the same language, in particular if they want to be able to cooperate efficiently. In this regard, it appears that the term "hybrid warfare" leads to less confusion than the term "hybrid threat(s)".

Facing up to contemporary conflictuality

Instead of focusing on a chameleon term, often leading to confusion in minds, the EU and NATO should usefully face up to contemporary conflictuality and admit that the current enemy is capable of combining the quantity that we no longer have and the quality that we think we still have. The emergence of the *buzz word* "hybrid warfare" can therefore be the occasion to redefine contemporary defence strategies and to consider the geopolitical phenomena in their full specificity and complexity. Indeed, the Western forces' overstretch, whether in internal or external operations, leads to a loss of know-how, whereas the probable adversary is gaining some. The technical-tactical excellence of Western countries' weapon systems and know-how is not sufficient anymore. It is therefore necessary to define a long-term strategy and to mobilise sufficient troops equipped with a proper know-how. In this context, it would be judicious to examine with attention and to answer adequately the following questions: is Russia really a threat to the EU or NATO? Does Moscow intend to attack with military and/or cybernetic means a Baltic State in order to test the solidarity of the West, and particularly the solidarity of NATO? If yes, are Western forces sufficiently powerful, equipped and manoeuvrable to respond efficiently and in a coordinated way? If no, can Russia be considered as a partner, in particular in countering terrorism? As for the organisation "Islamic State", is it in a position to endanger our critical infrastructures, including through the use of cyber terrorism? If yes, how could we improve our capability to detect the authors of cyber attacks? Would it be possible that we make ourselves less dependent on IT networks?

Responding efficiently to propaganda

How could we respond efficiently to propaganda? Should the EU and NATO not increase their workforce in order to be able to respond efficiently to disinformation, which has become a very complex phenomenon? Is civilian-military cooperation sufficient in this field? Accordingly, for instance, in order to prevent an external aggression coinciding with an insurgency – and without neglecting the possibility to resort to a military intervention –, should we not focus on the population's political and social demands, if they are not conflicting with our fundamental interests?

Continuously involving Belgium in the EU Centres of Excellence

The work of the "EU Fusion Cell", the NATO "Hybrid Analysis Branch" and the "European Centre of Excellence for countering hybrid threats" in Helsinki can help, on the one hand, to detect "hybrid threats" in gestation and, on the other hand, to determine their origin in order to respond in such a way that a hybrid campaign does not degenerate into a military conflict, but is contained and reduced before any escalation. The budget dedicated by the EU to countering hybrid danger could nevertheless be increased in order to enable the surveillance of a greater number of countries using hybrid warfare practices. Other Centres of Excellence, such as the centre specialised in cyber defence (located in Tallinn, Estonia) also have a leading role to play. Belgium's involvement in these individual organisations enables it to remain a credible partner for the EU and NATO, whereas Europe's environment fundamentally changed both in the aftermath of the Ukrainian crisis and due to the instability on its southern flank. In this regard, one can only encourage Belgium to join the signatory countries to the Memorandum of Understanding on the project of a research centre in Helsinki.

Eventually, Belgium could usefully develop a centralised policy taking into account its vital interests, its vulnerabilities and the comprehensive responses to counter hybrid campaigns.

Annexes

Annex 1: European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response" (6 April 2016)

1. INTRODUCTION

In recent years, the European Union's security environment has changed dramatically. Key challenges to peace and stability in the EU's eastern and southern neighbourhood continue to underscore the need for the Union to adapt and increase its capacities as a security provider, with a strong focus on the close relationship between external and internal security. Many of the current challenges to peace, security and prosperity originate from instability in the EU's immediate neighbourhood and changing forms of threats. In his 2014 Political Guidelines, the European Commission President Jean-Claude Juncker stressed the need 'to work on a stronger Europe when it comes to security and defence' and to combine European and national instruments in a more effective way than in the past. Further to this, following the invitation from the Foreign Affairs Council of 18 May 2015, the High Representative in close cooperation with Commission services and the European Defence Agency (EDA), and in consultation with the EU Member States, undertook work to present this joint framework with actionable proposals to help counter hybrid threats and foster the resilience of the EU and Member States, as well as partners.[1] In June 2015 the European Council recalled the need to mobilise EU instruments to help counter hybrid threats.[2]

While definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats.

Insofar as countering hybrid threats relates to national security and defence and the maintenance of law and order, the primary responsibility lies with Member States, as most national vulnerabilities are country-specific. However, many EU Member States face common threats, which can also target cross-border networks or infrastructures. Such threats can be addressed more effectively with a coordinated response at EU level by using EU policies and instruments, to build on European solidarity, mutual assistance and the full potential of the Lisbon Treaty. EU policies and instruments can and, to a significant degree already do, play a key value-adding role in building awareness. This is helping to improve the resilience of Member States to respond to common threats. The Union's external action proposed under this framework is guided by the principles set out in Article 21 of the Treaty on European Union (TEU), which include democracy, the rule of law, the universality and indivisibility of human rights and respect for the principles of the United Nations Charter and international law[3].

This Joint Communication aims to facilitate a holistic approach that will enable the EU, in coordination with Member States, to specifically counter threats of a hybrid nature by creating synergies between all relevant instruments and fostering close cooperation between all relevant actors.[4] The actions build on existing strategies and sectoral policies that contribute to achieving greater security. In particular, the European Agenda on Security[5], the upcoming European Union Global Strategy for foreign and security policy and European Defence Action Plan[6], the EU Cybersecurity Strategy[7], the

Energy Security Strategy[8], the European Union Maritime Security Strategy[9] are tools that may also contribute to countering hybrid threats.

As NATO is also working to counter hybrid threats and the Foreign Affairs Council proposed stepping up cooperation and coordination in this area, some of the proposals aim to enhance EU–NATO cooperation on countering hybrid threats.

The proposed response focuses on the following elements: improving awareness, building resilience, preventing, responding to crisis and recovering.

2. RECOGNISING THE HYBRID NATURE OF A THREAT

Hybrid threats aim to exploit a country's vulnerabilities and often seek to undermine fundamental democratic values and liberties. As a first step, the High Representative and the Commission will work together with Member States to enhance situational awareness by monitoring and assessing the risks that may target EU vulnerabilities. The Commission is developing security risk assessment methodologies to help inform decision makers and promote risk-based policy formulation in areas ranging from aviation security to terrorist financing and money laundering. In addition, a survey by Member States identifying areas vulnerable to hybrid threats would be pertinent. The aim would be to identify indicators of hybrid threats, incorporate these into early warning and existing risk assessment mechanisms and share them as appropriate.

Action 1: Member States, supported as appropriate by the Commission and the High Representative, are invited to launch a hybrid risk survey to identify key vulnerabilities, including specific hybrid related indicators, potentially affecting national and pan-European structures and networks.

3. ORGANISING THE EU RESPONSE: IMPROVING AWARENESS

3.1. EU Hybrid Fusion Cell

It is essential that the EU, in coordination with its Member States, has a sufficient level of situational awareness to identify any change in the security environment related to hybrid activity caused by State and/or non-state actors. To effectively counter hybrid threats, it is important to improve information exchange and promote relevant intelligence-sharing across sectors and between the European Union, its Member States and partners.

An EU Hybrid Fusion Cell will offer a single focus for the analysis of hybrid threats, established within the EU Intelligence and Situation Centre (EU INTCEN) of the European External Action Service (EEAS). This Fusion Cell would receive, analyse and share classified and open source information specifically relating to indicators and warnings concerning hybrid threats from different stakeholders within the EEAS (including EU Delegations), the Commission (with EU agencies[10]), and Member States. In liaison with existing similar bodies at EU[11] and at national level, the Fusion Cell would analyse external aspects of hybrid threats, affecting the EU and its neighbourhood, in order to rapidly analyse relevant incidents and inform the EU's strategic decision-making processes, including by providing inputs to the security risk assessments carried out at EU level. The Fusion Cell's analytical output would be processed and handled in accordance with the European Union classified information and data protection rules.[12] The Cell should liaise with existing bodies at EU and national level. Member States should establish National Contact Points connected to the EU Hybrid Fusion Cell. Staff inside and outside the EU (including those deployed to EU delegations, operations and missions) and in Member States should also be trained to recognise early signs of hybrid threats.

Action 2: Creation of an EU Hybrid Fusion Cell within the existing EU INTCEN structure, capable of receiving and analysing classified and open source information on hybrid threats. Member States are invited to establish National Contact Points on hybrid threats to ensure cooperation and secure communication with the EU Hybrid Fusion Cell.

3.2. Strategic communication

Perpetrators of hybrid threats can systematically spread disinformation, including through targeted social media campaigns, thereby seeking to radicalise individuals, destabilise society and control the political narrative. The ability to respond to hybrid threats by employing a sound strategic communication strategy is essential. Providing swift factual responses and raising public awareness about hybrid threats are major factors for building societal resilience.

Strategic communication should make full use of social media tools, as well as the traditional visual, audio and web-based media. The EEAS, building on the activities of the East and Arab StratCom Task Forces, should optimise the use of linguists fluent in relevant non-EU languages and social media specialists, who can monitor non-EU information and ensure targeted communication to react to disinformation. Furthermore, Member States should develop coordinated strategic communication mechanisms to support attribution and counter disinformation in order to expose hybrid threats.

Action 3: The High Representative will explore with Member States ways to update and coordinate capacities to deliver proactive strategic communications and optimise use of media monitoring and linguistic specialists.

3.3. Centre of Excellence for 'countering hybrid threats'

Building on the experience of some Member States and partner organisations[13], one or a network of multinational institutes could act as a Centre of Excellence addressing hybrid threats. Such a Centre could focus on researching how hybrid strategies have been applied, and could encourage the development of new concepts and technologies within the private sector and industry to help Member States build resilience. The research could contribute to aligning EU and national policies, doctrines and concepts, and to ensuring that decision-making can take account of the complexities and ambiguities associated with hybrid threats. Such a Centre should design programmes to advance research and exercises to find practical solutions to existing challenges posed by hybrid threats. The strength of such a Centre would rely on the expertise developed by its multinational and cross-sector participants from the civilian and military, private and academic sectors.

Such a Centre could work closely with existing EU[14] and NATO[15] centres of excellence in order to benefit from insights into hybrid threats that have been gained from cyber defence, strategic communication, civilian military cooperation, energy and crisis response.

Action 4: Member States are invited to consider establishing a Centre of Excellence for 'countering hybrid threats'.

4. ORGANISING THE EU RESPONSE: BUILDING RESILIENCE

Resilience is the capacity to withstand stress and recover, strengthened from challenges. To effectively counter hybrid threats, the potential vulnerabilities of key infrastructures, supply chains and society must be addressed. By drawing on the EU instruments and policies, infrastructure at the EU level can become more resilient.

4.1. Protecting critical infrastructure

It is important to protect critical infrastructures (e.g. energy supply chains, transport), since an unconventional attack by perpetrators of hybrid threats on any 'soft target' could lead to serious economic or societal disruption. To ensure protection of critical infrastructure, the European Programme for Critical Infrastructure Protection[16] (EPCIP) provides an all-hazard cross-sectoral systems approach, looking at interdependencies, based on the implementation of activities under the prevention, preparedness and response work streams. The Directive on European Critical Infrastructures[17] establishes a procedure for identifying and designating European Critical Infrastructures (ECI) and a common approach for assessing the need to improve their protection. In particular, work should be re-launched under the Directive to reinforce the resilience of critical infrastructures relating to transport (e.g. EU's main airports and merchant ports). The Commission will assess whether to develop common tools, including indicators, for improving resilience of critical infrastructure against hybrid threats in all relevant sectors.

***Action 5**: The Commission, in cooperation with Member States and stakeholders, will identify common tools, including indicators, with a view to improve protection and resilience of critical infrastructure against hybrid threats in relevant sectors.*

4.1.1. Energy Networks

Undisturbed production and distribution of power is of vital importance to the EU and significant power failures could be damaging. An essential element for countering hybrid threats is to further diversify EU's energy sources, suppliers and routes, in order to provide more secure and resilient energy supplies. The Commission is also carrying out risk and safety assessments ("stress tests") on EU power plants. To ensure energy diversification, work in the context of the Energy Union Strategy is being intensified: for example, the Southern Gas Corridor can enable gas from the Caspian region to reach Europe and in Northern Europe the establishment of liquid gas hubs with multiple suppliers. This example should be followed in Central and Eastern Europe and in the Mediterranean, where a gas hub is under development.[18] The developing market for liquefied natural gas will also contribute positively to this objective.

Concerning nuclear material and facilities, the Commission supports the development and adoption of the highest standards in safety thereby reinforcing resilience. The Commission is encouraging consistent transposition and implementation of the Nuclear Safety Directive[19] that sets rules on prevention of accidents and mitigation of accident consequences and of the provisions of the Basic Safety Standards Directive[20] on international cooperation on emergency preparedness and response, particularly between neighbouring Member States and with neighbouring countries.

***Action 6**: The Commission, in cooperation with Member States, will support efforts to diversify energy sources and promote safety and security standards to increase resilience of nuclear infrastructures.*

4.1.2 Transport and supply chain security

Transport is essential for the functioning of the Union. Hybrid attacks on transport infrastructure (such as airports, road infrastructures, ports and railways) can have serious consequences, leading to disruptions to travel and supply chains. In implementing aviation and maritime security legislation[21], the Commission carries out regular inspections[22] and, through its work on land transport security, aims to address emerging hybrid threats. In this context, an EU framework is being discussed under the revised Aviation Safety Regulation[23], as part of the Aviation Strategy for Europe[24]. Furthermore, threats to maritime security are being addressed in the European Union Maritime Security Strategy and its Action Plan[25]. The latter enables the EU and its Member States to comprehensively tackle maritime security challenges, including countering hybrid threats, through cross-sectoral cooperation between civilian and military actors to protect maritime critical infrastructure, the global supply chain, maritime trade and maritime natural and energy resources. The security of the international supply chain is also addressed in the European Union Customs Risk Management Strategy and Action Plan[26].

***Action 7**: The Commission will monitor emerging threats across the transport sector and will update legislation where appropriate. In implementing the EU Maritime Security Strategy and the EU Customs Risk Management Strategy and Action Plan, the Commission and the High Representative (within their respective compentences), in coordination with Member States, will examine how to respond to hybrid threats, in particular those concerning transport critical infrastructure.*

4.1.3 Space

Hybrid threats could target space infrastructures with multi-sectoral consequences. The EU has designed the Space Surveillance and Tracking support Framework[27] to network such assets owned by Member States in order to deliver Space Surveillance and Tracking services[28] to identified users (Member States, EU institutions, spacecraft owners and operators and civil protection authorities). In the context of the upcoming Space Strategy for Europe, the Commission will explore its further development, to monitor hybrid threats to space infrastructures.

Satellite communications (SatComs) are key assets for crisis management, disaster response, police, border and coastal surveillance. They are the backbone of large-scale infrastructures, such as transport, space or remotely piloted aircraft systems. In line with the European Council call to prepare the next generation of Governmental SatCom (GovSatCom), the Commission, in cooperation with the European Defence Agency, is assessing ways to pool demand, in the context of the upcoming Space Strategy and European Defence Action Plan.

Many critical infrastructures rely on exact timing information to synchronise their networks (e.g. energy and telecommunication) or timestamp transactions (e.g. financial markets). The dependency on a single Global Navigation Satellite System time synchronisation signal does not offer the resilience required to counter hybrid threats. Galileo, the European global navigation satellite system, would offer a second reliable timing source.

Action 8: Within the context of the upcoming Space Strategy and European Defence Action Plan, the Commission will propose to increase the resilience of space infrastructure against hybrid threats, in particular, through a possible extension of the Space Surveillance and Tracking scope to cover hybrid threats, the preparation for the next generation of GovSatCom at European level and the introduction of Galileo in critical infrastructures dependant on time synchronisation.

4.2. Defence capabilities

Defence capabilities need to be strengthened in order to enhance the EU's resilience to hybrid threats. It is important to identify the relevant key capability areas, e.g. surveillance and reconnaissance capabilities. The European Defence Agency could be a catalyst for a military capability development (for example, by shortening defence capability development cycles, investing in technology, systems and prototypes, opening defence business to innovative commercial technologies) related to hybrid threats,. Possible actions could be examined under the upcoming European Defence Action Plan.

Action 9: The High Representative, supported as appropriate by Member States, in liaison with the Commission, will propose projects on how to adapt defence capabilities and development of EU relevance, specifically to counter hybrid threats against a Member State or several Member States.

4.3. Protecting public health and food security

The population's health could be jeopardised by the manipulation of communicable diseases or the contamination of food, soil, air and drinking water by chemical, biological, radiological and nuclear (CBRN) agents. In addition, the intentional spreading of animal or plant diseases may seriously affect the food security of the Union and have major economic and social effects on crucial areas of the EU food chain. Existing EU structures for health security, environmental protection and for food safety can be used to respond to hybrid threats using these methods.

Under EU law on cross-border health threats[29], existing mechanisms coordinate preparedness for serious cross-border threats to health, linking Member States, EU agencies and Scientific Committees[30] through the Early Warning and Response System. The Health Security Committee, which coordinates Member States' response to threats, may act as a focal point on vulnerabilities in public health,[31] to enshrine hybrid threats (in particular bioterrorism) in crisis communication guidelines and in (crisis simulation) capacity-building exercises with Member States. In the area of food safety, through the Rapid Alert System for Food and Feed (RASFF) and the Common Risk Management System (CRMS) for customs, competent authorities exchange risk analysis information in order to monitor health risks posed by contaminated food. For animal and plant health, the review of the EU legal framework[32] will add new elements to the existing "toolbox"[33], to be better prepared also for hybrid threats.

Action 10: The Commission, in cooperation with Member States, will improve awareness of and resilience to hybrid threats within existing preparedness and coordination mechanisms, notably the Health Security Committee.

4.4. Cybersecurity

The EU greatly benefits from its interconnected and digitised society. Cyberattacks could disrupt digital services across the EU and such attacks could be used by perpetrators of hybrid threats. Improving the resilience of communication and information systems in Europe is important to support the Digital Single Market. The EU Cybersecurity Strategy and the European Agenda on Security provide the overall strategic framework for EU initiatives on cybersecurity and cybercrime. The EU has been active in developing awareness, cooperation mechanisms and responses under the Cybersecurity Strategy deliverables. In particular, the proposed Network and Information Security (NIS) Directive[34], addresses cybersecurity risks for a broad range of essential service providers in the fields of energy, transport, finance and health. These providers, as well as providers of key digital services (e.g. cloud computing) should take appropriate security measures and report serious incidents to national authorities, noting any hybrid characteristics. When adopted by the co-legislators, the effective transposition and implementation of the Directive would foster cybersecurity capabilities across Member States, reinforcing their cooperation on cybersecurity through information exchange and best practices on countering hybrid threats. In particular, the Directive provides for the establishment of a network of 28 national CSIRTs (Computer Security Incidents Response Teams) and CERT-EU[35] to pursue operational cooperation on a voluntary basis.

To encourage public-private cooperation and EU-wide approaches to cybersecurity, the Commission established the NIS Platform, which issues best practice guidance on risk management. While Member States determine security requirements and modalities to notify national incidents, the Commission encourages a high degree of convergence in risk management approaches, drawing in particular on the European Union Network and Information Security Agency (ENISA).

Action 11: The Commission encourages Member States as a matter of priority to establish and fully utilise a network between the 28 CSIRTs and the CERT-EU as well as a framework for strategic cooperation. The Commission, in coordination with Member States, should ensure that sectorial initiatives on cyber threats (e.g. aviation, energy, maritime) are consistent with cross-sectorial capabilities covered by the NIS Directive to pool information, expertise and rapid responses.

4.4.1. Industry

Increased reliance on cloud computing and big data has increased vulnerability to hybrid threats. The Digital Single Market Strategy provides for a contractual Public-Private Partnership on cybersecurity[36], which will focus on research and innovation and will help the Union to retain a high degree of technological capacity in this area. The contractual Public-Private Partnership will build trust among different market players and develop synergies between the demand and supply side. While the contractual Public-Private Partnership and accompanying measures will primarily focus on civilian cybersecurity products and services, the outcome of these initiatives should allow technology users to be better protected also against hybrid threats.

Action 12: The Commission, in coordination with Member States, will work together with industry within the context of a contractual Public Private Partnership for cybersecurity, to develop and test technologies to better protect users and infrastructures against cyber aspects of hybrid threats.

4.4.2. Energy

The emergence of smart homes and appliances and the development of the smart grid, increasing digitalisation of the energy system also results in an increased vulnerability to cyberattacks. The European Energy Security Strategy[37] and the Energy Union Strategy[38] support an all-hazard approach, in which resilience to hybrid threats is integrated. The Thematic Network on Critical Energy Infrastructure Protection fosters collaboration among operators in the energy sector (oil, gas, electricity). The Commission launched a web-based platform to analyse and share information on threats and incidents.[39] It is also developing, together with stakeholders[40], a comprehensive energy-sector strategy on cybersecurity in smart grid operations to reduce vulnerabilities. Whilst electricity markets are increasingly integrated, rules and procedures for how to deal with crisis situations are still

national. We need to ensure that governments co-operate with each other in preparing for and preventing and mitigating risks and that all relevant players act on the basis of a common set of rules.

***Action 13*: The Commission will issue guidance to smart grid asset owners to improve cybersecurity of their installations. In the context of the electricity market design initiative, the Commission will consider proposing 'risk preparedness plans' and procedural rules for sharing information and ensuring solidarity across Member States in times of crisis, including rules on how to prevent and mitigate cyber-attacks.**

4.4.3. Ensuring sound financial systems

The EU's economy needs a secure financial and payment system to function. Protecting the financial system and its infrastructure from cyber-attacks, irrespective of the motive or nature of the attacker, is essential. To deal with hybrid threats against EU financial services the industry needs to understand the threat, to have tested its defences and to have the necessary technology to protect the industry from attack. Accordingly, sharing information on threats among financial market participants and with relevant authorities and key service providers or customers is crucial but needs also to be secure and meet data protection requirements. In line with work in international fora, including the G7's work in this sector, the Commission will seek to identify factors that hinder the appropriate sharing of information on threats and propose solutions. It is important to ensure regular testing and refinement of protocols to protect business and relevant infrastructures, including continuous upgrading of security enhancing technologies.

***Action 14*: The Commission, in cooperation with ENISA[41], Member States, relevant international, European and national authorities and financial institutions, will promote and facilitate threat information-sharing platforms and networks and address factors that hinder the exchange of such information.**

4.4.4. Transport

Modern transport systems (rail, road, air, maritime) rely on information systems that are vulnerable cyber-attacks. Given the cross-border dimension, there is a particular role for the EU to play. The Commission, in coordination with Member States, will continue analysing cyber-threats and risks related to unlawful interferences with transport systems. The Commission is developing a Roadmap on cybersecurity for aviation in cooperation with the European Aviation safety Agency (EASA)[42]. Cyber threats to maritime security are also addressed in the European Union Maritime Security Strategy and its Action Plan.

***Action 15*: The Commission and the High Representative (within their respective areas of competence), in coordination with Member States, will examine how to respond to hybrid threats, in particular those concerning cyber-attacks across the transport sector.**

4.5. Targeting hybrid threat financing

Perpetrators of hybrid threats need financing to maintain their activities. Financing can be used to support terrorist groups or more subtle forms of destabilisation, such as supporting pressure groups and fringe political parties. The EU stepped up efforts against crime and terrorist financing, as set out in the European Agenda on Security, in particular with the Action Plan.[43] In this context, namely, the revised European anti-money laundering framework reinforces the fight against terrorist financing and money laundering, facilitates the work of national Financial Intelligence Units (FIUs) to identify and follow suspicious money transfers and information exchanges, while ensuring traceability of funds transfers in the European Union. It could therefore also contribute to countering hybrid threats. In the context of CFSP instruments, tailored and effective restrictive measures could be explored to counter hybrid threats.

***Action 16*: The Commission will use the implementation of the Action Plan on Terrorist Financing to also contribute to countering hybrid threats.**

4.6. Building resilience against radicalisation and violent extremism

Although terrorist acts and violent extremism are not *per se* of a hybrid nature, perpetrators of hybrid threats can target and recruit vulnerable members of society, radicalising them through modern channels of communication (including internet social media and proxy groups) and propaganda.

In order to tackle extremist content on the Internet, the Commission is – within the context of the Digital Single Market strategy – analysing the need for potential new measures, with due regard for their impact on the fundamental rights of freedom of expression and information. This could include rigorous procedures for removing illegal content, while avoiding the take down of legal content ('notice and action') and greater responsibility and due diligence by intermediaries in the management of their networks and systems. This would complement the existing voluntary approach, where internet and social media companies (in particular under the umbrella of the EU Internet Forum) and in cooperation with Europol's EU Internet Referral Unit, swiftly remove terrorist propaganda.

Within the context of the European Security Agenda, radicalisation is being countered by exchanging experiences and developing best practices, including cooperation in third countries. The Syria Strategic Communication Advisory Team aims to reinforce the development and dissemination of alternative messages to counter terrorist propaganda. The Radicalisation Awareness Network supports Member States and practitioners, who need to interact with radicalised individuals (including foreign terrorist fighters) or with those deemed vulnerable to radicalisation. The Radicalisation Awareness Network provides training activities and advice and will offer support to priority third countries, where there is willingness to engage. In addition, the Commission is fostering judicial cooperation between criminal justice actors, including Eurojust, to counter terrorism and radicalisation across Member States, including handling foreign terrorist fighters and returnees.

Complementing the above approaches in its external action, the EU contributes to countering violent extremism, including through external engagement and outreach, prevention (countering radicalisation and terrorist financing), as well as through measures to address underlying economic, political and societal factors that provide opportunities for terrorist groups to flourish.

Action 17: The Commission is implementing the actions against radicalisation set out in the European Agenda on Security and is analysing the need to reinforce procedures for removing illegal content, calling on intermediaries' due diligence in managing networks and systems.

4.7. Increasing cooperation with third countries

As underlined in the European Agenda on Security, the EU has increased its focus on building capacities in partner countries in the security sector, *inter alia*, by building on the nexus between security and development and developing the security dimension of the revised European Neighbourhood Policy[44]. These actions can also promote partners' resilience to hybrid activities.

The Commission intends to further intensify the exchange of operational and strategic information with enlargement countries and within the Eastern Partnership and Southern Neighbourhood as appropriate to help combat organised crime, terrorism, irregular migration and trafficking of small arms. On counter-terrorism, the EU is stepping up cooperation with third countries by establishing upgraded security dialogues and Action Plans.

EU external financing instruments aim at building functioning and accountable institutions in third countries[45] which are a prerequisite for responding effectively to security threats and for enhancing resilience. In this context, security sector reform and capacity building in support of security and development[46] are key tools. Under the Instrument contributing to Stability and Peace[47], the Commission has developed actions to enhance cyber-resilience and partners' abilities to detect and respond to cyber-attacks and cybercrime, which can counter hybrid threats in third countries. The EU is funding capacity building activities in partner countries to mitigate security risks linked to CBRN issues[48].

Finally, in the spirit of the comprehensive approach to crisis management, Member States could deploy Common Security and Defence Policy (CSDP) tools and missions, independently or to complement deployed EU instruments, in order to assist partners in enhancing their capacities. The

following actions could be considered: (i) support for strategic communication, (ii) advisory support for key ministries exposed to hybrid threats; (iii) additional support for border management in case of emergency. Further synergies could be explored between CSDP instruments and security, customs and justice actors, including the relevant EU agencies[49], INTERPOL and the European Gendarmerie Force, in accordance with their mandates.

***Action 18**: The High Representative, in coordination with the Commission, will launch a hybrid risk survey in neighbourhood regions.*

The High Representative, the Commission and Member States will use the instruments at their respective disposal to build partners' capacities and strengthen their resilience to hybrid threats. CSDP missions could be deployed, independently or to complement EU instruments, to assist partners in enhancing their capacities.

5. PREVENTING, RESPONDING TO CRISIS AND RECOVERING

As outlined in Section 3.1, the proposed EU Hybrid Fusion Cell aims to analyse relevant indicators to prevent and respond to hybrid threats and inform EU decision-makers. While liabilities can be mitigated through long term policies at national and EU level, in the short term it remains essential to strengthen the ability of Member States and the Union to prevent, respond and recover from hybrid threats in a swift and coordinated manner.

A rapid response to events triggered by hybrid threats is essential. In this respect, the facilitation of national civil protection actions and capacities by the European Emergency Response Coordination Centre[50] could be an effective response mechanism for aspects of hybrid threats requiring a civil protection response. This could be achieved in coordination with other EU response mechanisms and early warning systems, in particular with the EEAS Situation Room on external security dimensions and the Strategic Analysis and Response centre on internal security.

The solidarity clause (Article 222 of the TFEU) allows for Union action, as well as action between Member States, if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. Action by the Union to assist the Member State is implemented by applying Council Decision 2014/415/EU.[51] Arrangements for coordination within the Council should rely on the EU Integrated Political Crisis Response.[52] Under these arrangements, the Commission and the High Representative (in their respective areas of competence), identify relevant Union instruments and submits proposals to the Council for decisions on exceptional measures.

Article 222 TFEU also addresses situations that involve direct assistance by one or several Member States to a Member State that has experienced a terrorist attack or disaster. In this respect, Council Decision 2014/415/EU does not apply. Given the ambiguity associated with hybrid activities, the possible last resort applicability of the Solidarity Clause should be assessed by the Commission and the High Representative (in their respective areas of competence), in case an EU Member State is subject to significant hybrid threats.

By contrast to Article 222 TFEU, if multiple serious hybrid threats constitute armed aggression against an EU Member State, Article 42 (7) TEU could be invoked to provide an appropriate and timely response. A wide-ranging and serious manifestation of hybrid threats may also require increased cooperation and coordination with NATO.

When preparing their forces, Member States are encouraged to take potential hybrid threats into account. To be prepared to take decisions swiftly and effectively in case of a hybrid attack, Member States need to hold regular exercises, at working and political level, to test national and multinational decision-making ability. The objective would be to have a common operational protocol between Member States, the Commission and the High Representative, outlining effective procedures to follow in case of a hybrid threat, from the initial identification phase to the final phase of attack, and mapping the role of each Union institution and actor in the process.

As an important component of the CSDP, engagement could provide (a) civilian and military training, (b) mentoring and advisory missions to improve a threatened state's security and defence capacity, (c) contingency planning to identify signals of hybrid threats and strengthen early warning

capabilities, (d) support to border control management, in case of emergency, (e) support in specialised areas, such as CBRN risk mitigation and non-combatant evacuation.

***Action 19**: The High Representative and the Commission, in coordination with the Member States, will establish a common operational protocol and carry out regular exercises to improve strategic decision-making capacity in response to complex hybrid threats building on the Crisis Management and Integrated Political Crisis Response procedures.*

***Action 20**: The Commission and the High Representative, in their respective areas of competence, will examine the applicability and practical implications of Articles 222 TFEU and Article 42(7) TEU in case a wide-ranging and serious hybrid attack occurs.*

***Action 21**: The High Representative, in coordination with Member States, will integrate, exploit and coordinate the capabilities of military action in countering hybrid threats within the Common Security and Defence Policy.*

6. INCREASING COOPERATION WITH NATO

Hybrid threats represent a challenge not only for the EU but also for other major partner organisations including the United Nations (UN), the Organisation for Security and Cooperation in Europe (OSCE) and particularly NATO. An effective response calls for dialogue and coordination both at political and operational level between organisations. Closer interaction between the EU and NATO would make both organisations better able to prepare and respond to hybrid threats effectively in a complementary and mutually supporting manner based on the principle of inclusiveness, while respecting each organisation's decision-making autonomy and data protection rules.

The two organisations share values and face similar challenges. EU Member States and NATO Allies alike expect their respective organisations to support them, acting swiftly, decisively and in a coordinated manner in the event of a crisis, or ideally to prevent the crisis from happening. A number of areas for closer EU–NATO cooperation and coordination have been identified, including situational awareness, strategic communications cybersecurity and crisis prevention and response. The ongoing informal EU–NATO dialogue on hybrid threats should be strengthened in order to synchronise the two organisations' activities in this area.

In order to develop complementary EU/NATO responses, it is important that both share the same situational awareness picture before and during crisis. This could be done through regular sharing of analyses and lessons identified, but also through direct liaison between the EU Hybrid Fusion Cell and NATO's hybrid cell. It is equally important to build mutual awareness of each other's respective crisis management procedures to ensure swift and effective reactions. Resilience could be enhanced by ensuring complementarity in setting benchmarks for critical parts of their infrastructures, as well as close collaboration in strategic communication and cyber defence. Fully inclusive joint exercises both at political and technical levels would enhance the effectiveness of the two organisations' respective decision-making capacity. Exploring further options in training activities would help develop a comparable level of expertise in critical areas.

***Action 22**: The High Representative, in coordination with the Commission, will continue informal dialogue and enhance cooperation and coordination with NATO on situational awareness, strategic communications, cybersecurity and "crisis prevention and response" to counter hybrid threats, respecting the principles of inclusiveness and autonomy of each organisation's decision making process.*

7. CONCLUSIONS

This Joint Communication outlines actions designed to help counter hybrid threats and foster the resilience at the EU and national level, as well as partners. As the focus is on improving awareness, it is proposed to establish dedicated mechanisms to exchange information with Member States and to coordinate the EU's capacity to deliver strategic communications. Actions have been outlined to build resilience in areas such as cybersecurity, critical infrastructure, protecting the financial system from

illicit use and efforts to counter violent extremism and radicalisation. In each of these areas, implementation of agreed strategies by the EU and the Member States, as well as Member States' full implementation of existing legislation will be a key first step, while some more concrete actions have been put forward to further reinforce these efforts.

As regards preventing, responding to and recovering from hybrid threats, it is proposed to examine the feasibility of applying the Solidarity Clause Article 222 TFEU (as specified in the relevant Decision) and Art. 42(7) TEU, in case a wide-ranging and serious hybrid attack occurs. Strategic decision making capacity could be enhanced by establishing a common operational protocol.

Finally, it is proposed to step up cooperation and coordination between the EU and NATO in common efforts to counter hybrid threats.

In implementing this Joint Framework, the High Representative and the Commission are committed in mobilising relevant EU instruments at their respective disposal. It is important for the EU, together with the Member States, to work to reduce risks associated with exposure to potential hybrid threats from state and non-state actors.

Notes:

1. Council Conclusions on Common Defence and Security Policy (CSDP), May 2015 [Consilium 8971/15].

2. European Council Conclusions, June 2015 [EUCO 22/15].

3. The Charter of Fundamental Rights of the EU is binding on the institutions and on the Member States when they implement Union law.

4. Possible legislative proposals will be subject to Commission better regulation requirements, in line with Commission's Better Regulation Guidelines [SWD(2015) 111].

5. COM(2015) 185 final.

6. To be presented in 2016.

7. EU Cyber Defence Policy Framework [Consilium 15585/14] and Joint Communication on 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', February 2013 [JOIN(2013) 1].

8. Joint Communication on 'European Energy Security Strategy', May 2014 [SWD(2014) 330].

9. Joint communication 'For an open and secure global maritime domain: elements for a European Union maritime security strategy — JOIN(2014) 9 final — 06/03/2014.

10. In accordance with their mandates.

11. For example, Europol's European Cybercrime Centre and Counter Terrorism Centre, Frontex, EU Computer Emergency Response Team (CERT-EU).

12. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

13. NATO Centres of Excellence.

14. E.g. EU Institute for Security Studies (EU ISS), thematic EU Centres of Excellence on CBRN issues.

15. http://www.nato.int/cps/en/natohq/topics_68372.htm.

16. Communication from the Commission on a European Programme for Critical Infrastructure Protection, 12.12.2006, COM(2006) 786 final.

17. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345 of 23.12.2008.

18. On the progress achieved so far, see the State of the Energy Union 2015 (COM(2015) 572 final).

19. Council Directive 2009/71/Euratom of 25 June 2009 establishing a Community framework for the nuclear safety of nuclear installations, as amended by Council Directive 2014/87/Euratom of 8 July 2014.

20. Council Directive 2013/59/Euratom of 5 December 2013 laying down basic safety standards for the protection against the dangers arising from exposure to ionising radiation and repealing Directives 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom and 2003/122/Euratom.

21. Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002; Commission Implementing Regulation (EU) No 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security; Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security; Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security.

22. Under EU law, the Commission is required to carry out inspections to ensure Member States' correct implementation of aviation and maritime security requirements. This includes inspections of the appropriate authority in the Member State, as well as inspections at airports, ports, air carriers, ships and entities implementing security measures. The Commission inspections aim to ensure that EU standards are fully implemented by Member States.

23. Commission Regulation (EU) 2016/4 of 5 January 2016 amending Regulation (EC) No 216/2008 of the European Parliament and of the Council as regards essential requirements for environmental protection; Regulation (EC) No 216/2008 of 20/02/2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency.

24. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: An Aviation Strategy for Europe, COM/2015/0598 final, 7.12.2015.

25. In December 2014, the Council adopted an Action Plan to implement the European Union Maritime Security Strategy; http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf.

26. Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the EU Strategy and Action Plan for customs risk management: Tackling risks, strengthening supply chain security and facilitating trade, COM (2014) 527 final.

27. See Decision 541/2014 of the European Parliament and of the Council.

28. Such as in-orbit collision avoidance warning, alerts regarding breakup or collision and risky re-entries of space objects into the Earth's atmosphere.

29. Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC, OJ L 293/1, 05.11.2013.

30. Commission Decision C(2015) 5383 of 7.8.2015 on establishment of Scientific Committees in the field of public health, consumer safety and the environment.

31. in line with Decision 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC, OJ L 293/1.

32. Regulation 2016/429 of the European Parliament and of the Council on transmissible animal diseases and amending and repealing certain acts in the area of animal health ("Animal Health Law"), OJ L84), 31/3/2016. Concerning the Regulation of the European Parliament and of the Council on Protective measures against pests (“Plant Health Law”), a political agreement on the text has been reached by the European Parliament and the Council on 16 December 2015.

33. E.g. EU vaccine banks, sophisticated electronic animal disease information system, increased obligation for measures by labs and other entities dealing with pathogens.

34. Commission proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union COM(2013) 48 final - 7/2/2013. Political agreement has been reached by the Council of the EU and the European Parliament on this proposed Directive and the Directive should be formally adopted soon.

35. Computer Emergency Response Team (CERT-EU) for the EU institutions.

36. To be launched in mid-2016.

37. Communication from the Commission to the European Parliament and the Council: European Energy Security Strategy - COM/2014/0330 final.

38. Communication on 'A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy - COM/2015/080 final.

39. Incident and Threat Information Sharing EU Centre – ITIS.

40. In the form of the Energy Expert CyberSecurity Platform (EECSP).

41. European Union Network and Information Security Agency.

42. The new EASA regulation is currently under discussion between the European Parliament and the Council following the Commission's proposal on December 2015. Proposal for a regulation of the European Parliament and of the Council on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and repealing Regulation (EC) No 216/2008 of the European Parliament and of the Council- COM(2015) 613 final, 2015/0277 (COD).

43. Communication from the Commission to the European Parliament and the Council on an Action Plan for strengthening the fight against terrorist financing - (COM(2016) 50 final).

44. Joint Communication to the European Parliament, the Council, the European economic and social Committee and the Committee of the regions, Review of the European Neighbourhood Policy, 18.11.2015, JOIN(2015) 50 final.

45. Idem; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU Enlargement Strategy, 10.11.2015, COM(2015) 611 final; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Increasing the impact of EU Development Policy: an Agenda for Change, 13.10.2011, COM(2011) 637 final.

46. Joint Communication 'Capacity-building in support of security and development-enabling partners to prevent and manage crises (JOIN(2015)17final).

47. Regulation (EU) No 230/2014 of the European Parliament and of the Council of 11 March 2014 establishing an instrument contributing to stability and peace, OJ L 77/1, 15.3.2014.

48. Areas covered include border monitoring, crisis management, first response, illicit trafficking export control of dual-use items, disease surveillance and control, nuclear forensics, post incident recovery and protection of high-risk facilities. Best practices derived from tools developed within the EU CBRN Action Plan, such as the European nuclear security training centre and the EU's participation in International Border Monitoring Working Group, can be shared with third countries.

49. EUROPOL, FRONTEX, CEPOL, EUROJUST

50. http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en.

51. Council Decision 2014/415/EU on the arrangements for the implementation by the Union of the solidarity clause, OJ L 192, 1.7.2014, p. 53.

52. http://www.consilium.europa.eu/en/documents-publications/publications/2014/eu-ipcr/

Annex 2: European Commission, Joint Report to the European Parliament and the Council on the implementation of the "Joint Framework on countering hybrid threats: a European Union response" (19 July 2017)

1. INTRODUCTION

The EU is facing one of the greatest security challenges in its history. Threats are increasingly taking non-conventional forms, some physical such as new forms of terrorism, some using the digital space with complex cyber-attacks. Others are more subtle and are aimed at the coercive application of pressure including misinformation campaigns, and media manipulation. They seek to undermine core European values, such as human dignity, freedom and democracy. Recent coordinated cyber-attacks across the globe, for which attribution has proved challenging, have demonstrated the vulnerabilities of our societies and institutions.

In April 2016, the European Commission and the High Representative adopted a Joint Communication on countering hybrid threats[1] (Joint Framework). Recognising the trans-boundary and complex nature of hybrid threats this Framework proposes a whole-of-government approach to strengthening the overall resilience of our societies. The Council[2] welcomed the initiative and the proposed actions, and invited the Commission and the High Representative to report on progress in July 2017. While the EU can assist Member States to build their resilience against hybrid threats, the primary responsibility lies with Member States, insofar as countering hybrid threats relates to national security and defence.

This Joint Framework for Countering Hybrid Threats forms an important part of the EU's overall more integrated approach to security and defence. It contributes to the creation of a Europe that protects, as called for by President Juncker in the State of the Union speech of September 2016. In 2016, the European Union also laid the foundations for a stronger European defence policy to address citizens' expectations for more protection. The EU Global Strategy for EU Foreign and Security policy[3] elaborated the need for an integrated approach to link internal resilience with EU's external actions, and called for synergies between defence policy and policies covering the internal market, industry, law enforcement and intelligence services. Following the adoption in November 2016 of the European Defence Action Plan, the Commission put forward concrete initiatives which will contribute to strengthening the EU's capacity to respond to hybrid threats by fostering resilience in the defence supply chains and reinforcing the single market for defence. In particular, on 7 June 2017, the Commission launched the European Defence Fund with proposed funding of €600m up to 2020 and €1.5bn annually post 2020. The Security Union Communication[4] recognised the need to counter hybrid threats and the importance of ensuring greater coherence between internal and external actions in the field of security.

EU leaders have placed security and defence at centre-stage in the debate about the future of Europe.[5] This was acknowledged in the Rome Declaration of 25 March 2017 which set out a vision of a safe and secure Union committed to strengthening its common security and defence. The Presidents of the European Council, the European Commission and the Secretary-General of NATO signed a Joint Declaration in Warsaw on 8 July 2016 with a view to giving new impetus and new substance to the EU-NATO strategic partnership. The Joint Declaration outlined seven concrete areas, including countering hybrid threats, where cooperation between the two organisations should be enhanced. A common set of 42 proposals for implementation was subsequently endorsed by both the EU and NATO Councils and a first report, showing substantial progress, was issued in June 2017[6].

The Commission's reflection paper on the future of European Defence[7] presented in June 2017 outlines different scenarios on how to address the growing security and defence threats facing Europe and enhance Europe's own abilities in defence by 2025. In all three scenarios security and defence are considered as integral elements of the European project, in order to protect and promote our interests at home and abroad. Europe must become a security provider and ensure progressively its own security.

No single Member State can face the challenges ahead on its own, in particular that of countering hybrid threats. Cooperation on defence and security is therefore not an option; it is a necessity to deliver on a Europe that protects.

The aim of this Report is to give an account of progress and next implementing steps on the actions in the four areas proposed in the Joint Framework: improving situational awareness; building resilience; strengthening the ability of Member States and the Union to prevent and respond to crisis, and for coordinated recovery; and enhance cooperation with NATO to ensure complementarity of measures. It should be read in conjunction with the monthly progress reports towards an effective and genuine Security Union.

2. RECOGNISING THE HYBRID NATURE OF A THREAT

Hybrid activities are becoming a frequent feature of the European security environment. The intensity of these activities is increasing with growing concerns over elections being interfered with, disinformation campaigns, malicious cyber activities and perpetrators of hybrid acts trying to radicalise vulnerable members of society as their proxy actors. Vulnerabilities to hybrid threats are not limited to national boundaries. Hybrid threats need a coordinated response also at EU and NATO levels. Developments since April 2016 show that even though threats are often still assessed in isolation, there is a growing recognition and understanding within the Union of the hybrid nature of some of the activities observed and the need for coordinated action. The EU will continue its efforts to improve situational awareness and cooperation.

Action 1: Member States, supported as appropriate by the Commission and the High Representative, are invited to launch a hybrid risk survey to identify key vulnerabilities, including specific hybrid related indicators, potentially affecting national and pan-European structures and networks.

The Council has established a "Friends of the Presidency" group bringing together experts from Member States to build a generic survey that would enable them to better identify key indicators of hybrid threats, incorporate these into early warning and existing risk assessment mechanisms and share them as appropriate. Terms of Reference have been agreed and work has already started. The generic survey should be ready by the end of 2017 with the actual surveys commencing thereafter. Protection against hybrid threats should be mutually reinforcing. Member States are therefore encouraged to carry out these surveys as rapidly as possible as they will provide valuable information on the extent of vulnerability and preparedness across Europe.

a. IMPROVING AWARENESS

The sharing of intelligence analysis and assessment work is a key tool reducing uncertainty and enhancing situational awareness. Significant progress has been made over the past year. The EU Hybrid Fusion Cell has been established and is now fully operational, the East StratCom Task Force is in place and Finland has launched the European Centre for Countering Hybrid Threats. Much work has been focussed on analysing the tools and levers in disinformation or propaganda, with good cooperation existing between the EU StratCom Task Force East, the Hybrid Fusion Cell and NATO. This forms a good basis to continue building a more deeply-engrained culture of analysing and assessing threats to our internal and external security through a hybrid lens.

Hybrid Fusion Cell

Action 2: Creation of an EU Hybrid Fusion Cell within the existing EU Intelligence and Situation Centre structure, capable of receiving and analysing classified and open source information on hybrid threats. Member States are invited to establish National Contact Points on hybrid threats to ensure cooperation and secure communication with the EU Hybrid Fusion Cell.

The EU Hybrid Fusion Cell has been established within the EU Intelligence and Situation Centre to receive and analyse classified and open source information from different stakeholders concerning hybrid threats. Analysis is then shared within the EU and amongst Member States and in turn informs the EU decision-making processes, including inputs to the security risk assessments carried out at EU level. The EU Military Staff Intelligence Directorate contributes to the Fusion Cell work with

military analysis. To date, over 50 assessments and briefings on hybrid topics have been produced. Since January 2017, the Cell has produced a periodical "Hybrid Bulletin", analysing current threats and hybrid issues, shared directly within the EU institutions and bodies and national points of contact[8]. The Cell's Full Operating Capacity has been achieved, as planned, in May 2017. Finally, staff-to-staff engagement with NATO's nascent Hybrid Analysis Branch is ongoing, both in regard to sharing lessons learnt in the creation of the Fusion Cell and in sharing information (carried out in full respect of the EU rules on classified information exchange). The EU Hybrid Fusion Cell is currently identifying further initiatives to enhance future cooperation and will play a key role in the EU-NATO parallel exercises planned for autumn 2017 where the responsiveness of the EU Hybrid Fusion Cell will be tested and lessons identified will be incorporated.

Strategic communication

Action 3: The High Representative will explore with Member States ways to update and coordinate capacities to deliver proactive strategic communications and optimise use of media monitoring and linguistic specialists.

In recent months, increased disinformation campaigns and systematic spreading of fake news in social media is among a spectrum of measures used to undermine adversaries. Where social media is the preferred platform, information that appears reliable and legitimate can change public opinion for the benefit some individuals, organisations or governments. These hybrid tactics have a broader goal of creating confusion in our societies and discrediting democratic governments and our structures, institutions and elections. Fake news is often spread through online platforms (see also action 17). The Commission and the High Representative welcome recent steps taken by online platforms and news media publishers to tackle misinformation. The Commission will continue to encourage such voluntary measures.

The High Representative has put in place the East StratCom Task Force which forecasts and responds to disinformation cases and campaigns. This is significantly improving communication on Union policies in the Eastern Neighbourhood while also strengthening the media environment in these countries. The Task Force has over the past two years uncovered over 3,000 individual disinformation cases in 18 languages. The upcoming launch of a new website: *"#EUvsdisinformation*" with an online search facility will significantly improve user access. However, research and analytical work show that the number of disinformation channels and messages spread on a daily basis is significantly higher. The EU-STRAT project, funded by Horizon 2020, analyses policy and media in the Eastern Partnership countries.

The High Representative invites Member States to support the work of the StratCom Task Forces in order to counter more effectively the rise of hybrid threats. This will help the Task Force South to improve communication and outreach to the Arab World including in Arabic, myth-busting and establishing the facts about the European Union and its policies. Interaction with local journalists will help ensure the news products are culturally in tune. Both Task Forces, supported by the EU Hybrid Fusion Cell aim to support and complement Member States' related efforts. In addition, the Commission co-funds the European Strategic Communications Network, a collaborative network of 26 Member States that shares analysis, good practice and ideas on the use of strategic communications in Countering Violent Extremism, including on disinformation.

Centre of Excellence for 'countering hybrid threats'

Action 4: Member States are invited to consider establishing a Centre of Excellence for 'countering hybrid threats'.

Responding to the call to establish a Centre of Excellence, in April 2017, Finland launched the European Centre for Countering Hybrid Threats. Ten EU Member States[9], Norway and the USA are members, while both the European Union and NATO have been invited to support the steering board.[10] The Centre's mission is to encourage strategic dialogue as well as, conduct research and analysis working with communities of interest to improve resilience and ability to respond, in order to help counter hybrid threats. The Centre is expected to serve also as a venue for future hybrid exercises. The Centre has already established close contact with the EU Hybrid Fusion Cell and the work of the two

organisations should complement each other. The EU is currently assessing ways in which it can provide concrete support to the Centre.

b. BUILDING RESILIENCE

The Joint Framework places resilience (e.g. of transport, communications, energy, finance, or regional security infrastructures) at the heart of the EU action in order to resist propaganda and information campaigns, attempts to undermine business, societies and economic flows, as well as attacks on information technology and cyber-related infrastructure. It considers strengthening resilience as a preventive and deterrent action to solidify societies and avoid escalation of crises both within and outside the EU. The EU's added value lies in assisting Member States and partners to build their resilience, relying on a wide range of existing instruments and programmes. Significant progress has been made in actions to build resilience, in areas such as cybersecurity, critical infrastructure, protecting the financial system from illicit use and efforts to counter violent extremism and radicalisation.

Protecting critical infrastructure

Action 5: The Commission, in cooperation with Member States and stakeholders, will identify common tools, including indicators, with a view to improve protection and resilience of critical infrastructure against hybrid threats in relevant sectors.

In the context of the European Programme for Critical Infrastructure Protection (EPCIP), the Commission took forward the work to identify common tools, including vulnerability indicators, to improve resilience of critical infrastructure against hybrid threats in relevant sectors. In May 2017, the Commission organised a workshop on hybrid threats to critical infrastructure, in which participants included almost all Member States, operators of critical infrastructure, the EU Hybrid Fusion Cell and NATO as observer. A common roadmap and steps for the future work, based on a questionnaire sent to national authorities in the Member States was agreed. The Commission will further consult stakeholders in the autumn, with the aim of agreeing on indicators by the end of 2017.

The European Defence Agency is working to identify common capability and research shortfalls arising from the nexus of energy infrastructures and defence capabilities. The European Defence Agency will develop a conceptual paper in autumn 2017 as well as pilot actions for holistic methodologies.

Increasing the EU energy security of supply

Action 6: The Commission, in cooperation with Member States, will support efforts to diversify energy sources and promote safety and security standards to increase resilience of nuclear infrastructures.

The Commission made concrete proposals in the security of supply package in December 2016 and in April 2017, the Council and the European Parliament reached an agreement on the new security of gas supply regulation, which aims at preventing gas supply crises. The new rules will ensure a regionally coordinated and common approach to security of supply measures among the Member States. This will put the EU in a better position to prepare for and manage gas shortages, in case of a crisis or a hybrid attack. For the first time, the solidarity principle will apply: Member States will be able to help neighbours in the event of a serious crisis or attack, so that European households and businesses do not suffer black-outs.

The EU has also made progress in developing key projects to diversify its routes and sources of energy supplies, in line with the Energy Union Framework Strategy and the European Energy Security Strategy. For example, on the Southern Gas Corridor, concrete construction works are ongoing on all major pipeline projects: expansion of the South Caucasus pipeline, Trans-Anatolian and Trans-Adriatic pipelines, the upstream Shah Deniz II, as well as the expansion of the Southern Gas Corridor to Central Asia, notably Turkmenistan. Imports of liquefied natural gas (LNG) into Europe are increasing and are coming from new sources, such as the US. The example of the terminal in Lithuania shows how diversification projects can reduce the dependence on a single supplier. Strengthening energy efforts and better using indigenous energy sources, in particular renewables, also contributes to the diversification of energy routes and sources.

In the area of nuclear safety, the Commission is actively supporting, notably through workshops with national authorities and regulators, a consistent and effective implementation of the two Directives on nuclear safety and basic safety standards, which Member States are required to transpose by end of 2017 and 2018 respectively. Furthermore, the Euratom Research and Training programme contributes to increasing nuclear safety.

Transport and supply chain security

Action 7: The Commission will monitor emerging threats across the transport sector and will update legislation where appropriate. In implementing the EU Maritime Security Strategy and the EU Customs Risk Management Strategy and their Action Plans, the Commission and the High Representative (within their respective competences), in coordination with Member States, will examine how to respond to hybrid threats, in particular those concerning transport critical infrastructure.

In line with the Security Union communication, the Commission is facilitating security risk assessments at EU level with Member States, EU Intelligence and Situation Centre and relevant Agencies to identify threats to transport security and to support the development of effective and proportionate mitigation measures. The downing of Malaysia Airlines flight MH17 over Eastern Ukraine in 2014 highlighted the risk posed by the overflight of conflict zones. In line with the recommendations of the European High Level Task Force on Conflict Zones[11], the Commission developed a methodology for "common EU risk assessment" with the support of national aviation and security experts and the EEAS, allowing for the exchange of classified information and the definition of a common risk picture. In March 2017, the European Aviation Safety Agency (EASA) issued the first "Conflict Zones Information Bulletin"[12], on the basis of the results of this common EU risk assessment. The Commission is considering the extension of risk assessment activities carried out in the field of aviation security to other transport modes (e.g. rail, maritime) and proposals will be made in 2018. In June 2017, the Commission, EEAS, and Member States have launched a risk assessment exercise on railway security to identify gap and possible measures to mitigate the risks.

Considerable efforts on aviation security and Air Traffic Management (ATM) have also been made in the 7th Framework Programme and Horizon 2020 security research projects. In the field of civil aviation, the Commission, with the European Aviation Safety Agency and stakeholders, is developing two new initiatives to reinforce cyber-security, also tackling hybrid threats: the establishment of the Computer Emergency Response Team on Aviation, and the setting up of a Task Force on Cyber-security in Single European Sky Air Traffic Management Research (SESAR) Joint Undertaking, responsible for the Single European Sky Air Traffic Management. The European Defence Agency provides military inputs with regard to Aviation Cyber to SESAR Joint Undertaking, as well as to the European Aviation Safety Agency through the “European Strategic Coordination Platform on Cyber Security” which, at the request of Member States and industry, will help coordination at EU level of all activities in aviation. In line with the Roadmap on cybersecurity in aviation, in 2016 the European Aviation Safety Agency carried out gap analyses of existing rules and in particular the definition and establishment of the European Centre for Cybersecurity in Aviation; the latter is now operational and cooperates with the Computer Emergency Response Team-EU (CERT-EU) (Memorandum of Understanding signed in February 2017) producing threat analyses in aviation and with EUROCONTROL (a roadmap for cooperation adopted), while a website for distribution of open sources analyses was developed. By autumn 2017, a standardisation programme and a secured information exchange will be adopted.

Customs risk management

From a customs perspective, the Commission is focusing on significantly upgrading the advance cargo information and customs risk management system. This covers the full range of customs risks, including in relation to threats to the security and integrity of international supply chains and to relevant critical infrastructures (e.g. direct threats to sea-port facilities, airports or land borders posed by imports). The upgrading aims to ensure that customs in the EU obtain all necessary information from traders as regards the movement of goods; that they are able to share this information more effectively between Member States; that they apply common as well as Member State specific risk rules; and that they are able to target risky consignments more effectively by cooperating more intensively with other

authorities in particular other law enforcement and security agencies. The IT development required to implement this upgrading by the Commission is currently in its inception phase and relevant investments at central level will be launched in the coming months.

Space

Action 8: Within the context of the Space Strategy and European Defence Action Plan, the Commission will propose to increase the resilience of space infrastructure against hybrid threats, in particular, through a possible extension of the Space Surveillance and Tracking scope to cover hybrid threats, the preparation for the next generation of GovSatCom at European level and the introduction of Galileo in critical infrastructures dependant on time synchronisation.

The Commission, when preparing the regulatory framework on Government Satellite Communications (GovSatCom) and Space Surveillance and Tracking in 2018, will integrate resilience aspects against hybrid threats in its assessment. In line with the Space Strategy, when preparing the evolution of Galileo and Copernicus, the Commission, will assess the potential of these services to help mitigate vulnerability of critical infrastructures. The Evaluation report should be ready in autumn 2017 and the proposal on the next generation of Copernicus and Galileo in 2018. The European Defence Agency is working on collaborative capability development projects in the areas of space-based communications, military positioning, navigation and timing and earth observation. All projects will focus on resilience requirements in light of current and emerging hybrid threats.

Defence capabilities

Action 9: The High Representative, supported as appropriate by Member States, in liaison with the Commission, will propose projects on how to adapt defence capabilities and development of EU relevance, specifically to counter hybrid threats against a Member State or several Member States.

In 2016 and 2017, the European Defence Agency conducted three Table Top Exercises on hybrid threats scenarios, together with the Commission, EEAS and Member States' experts. Their findings will feed into the review of the Capability Development Plan, so that the resulting key capability developments required to counter hybrid threats will be integrated in the new EU capability development priorities. Work on the revision of the Requirements Catalogue 2005 will take account of the hybrid threat dimension. In April 2017, the European Defence Agency finalised an analysis report on military implications stemming from hybrid attacks directed against critical harbour infrastructure, which will be discussed in a workshop with maritime experts in October 2017. Another specific analysis of the military role in the context of countering mini-drones is scheduled for 2018. Furthermore, capabilities priorities to strengthen resilience against hybrid threats identified by Member States might also be eligible for support under the European Defence Fund as of 2019. The Commission calls on the co-legislators to ensure a swift adoption, and on Member States to submit proposals for capability projects to strengthen the EU resilience against hybrid threats.

Action 10: The Commission, in cooperation with Member States, will improve awareness of and resilience to hybrid threats within existing preparedness and coordination mechanisms, notably the Health Security Committee.

With a view to strengthening preparedness and resilience to hybrid threats, including capacity building within health and food systems, the Commission supports the Member States -through training, simulation exercises, and by facilitating exchange of experience guidelines and financing Joint Actions. This takes place notably under the EU health security framework on serious cross-border threats to health and under the Public Health Programme to implement the International Health Regulations, a legislative pillar, binding on 196 countries including the Member States, which aims to prevent and respond to acute public, cross-border health risks worldwide. To test cross-sectorial preparedness and response in the health sector, the Commission services will carry out an exercise on complex and multidimensional hybrid threats in the autumn of 2017. The Commission and the Member States are preparing a Joint Action on vaccination, including vaccine supply and demand forecasting and research on innovative vaccine manufacturing processes with a view to strengthening vaccine supply and improving health security at the EU level (2018-2020). The Commission also collaborates with the

European Food Safety Authority and the European Centre for Disease Prevention and Control to adapt to advanced scientific investigation techniques, for a more precise identification and sourcing of health threats, and a resulting rapid management of food safety outbreaks. The Commission established a network of research funders -Global Research Collaboration for Infectious Disease Preparedness – for coordinated research response within 48 hours of any significant outbreak.

***Action 11*: The Commission encourages Member States as a matter of priority to establish and fully utilise a network between the 28 CSIRTs and the CERT-EU (Computer Emergency Response Team-EU) as well as a framework for strategic cooperation. The Commission, in coordination with Member States, should ensure that sectorial initiatives on cyber threats (e.g. aviation, energy, maritime) are consistent with cross-sectorial capabilities covered by the NIS Directive to pool information, expertise and rapid responses.**

The recent global cyberattacks using ransomware and malware to disable thousands of computer systems have again highlighted the urgent need to step up cyber resilience and security actions within the EU. As announced in the Digital Single market mid-term review, the Commission and the High Representative are now reviewing the 2013 EU Cybersecurity Strategy, in particular through the adoption of a package planned for September 2017. The objective will be to provide a more effective cross-sector response to these threats, increasing trust in the digital society and economy. It will also review the mandate of ENISA the EU Agency for Network and Information Security, to define its role in the changed cybersecurity ecosystem. The European Council[13] welcomed the Commission's intention to review the Cybersecurity Strategy.

The adoption of the Network Information Services (NIS) Directive[14] in July 2016 was a key step towards building European level cybersecurity resilience. The Directive sets the first EU-wide rules on cybersecurity, improves cybersecurity capabilities and strengthens cooperation between Member States. It also requires companies in critical sectors to take appropriate security measures and to notify any serious cyber incidents to the relevant national authority. These sectors include energy, transport, water, healthcare, banking and financial market infrastructure. Online marketplaces, cloud computing services and search engines will have to take similar steps. Consistent implementation across different sectors, as well as across borders will be ensured by the Network Information Services Cooperation Group (established by the Commission in 2016), which is tasked with avoiding market fragmentation. In this context, the Network Information Services Directive is considered the reference framework for any sectorial initiatives in the area of cybersecurity. Furthermore, the Directive creates the Network of Computer Security Incident Response Teams (CSIRT), which gathers all relevant stakeholders. In parallel, the Commission and CERT-EU actively monitor the cyber threat landscape and exchange information with national authorities to ensure that the EU institutions Information Technology systems are secure and resilient to cyberattack. The May 2017 WannaCry ransomware incident presented the first opportunity for the Network to engage in operational information exchange and cooperation by means of dissemination of advice. The EU Computer Emergency Response Team was in close contact with the European Cybercrime Centre (EC3) at Europol, affected countries' Computer Security Incident Response Teams (CSIRTs), cybercrime units and key industry partners to mitigate the threat and assist victims. Exchanging national situational reports produced a common situational awareness across the EU. This experience allowed the Network to be better prepared for the next incidents (e.g. "NonPetya"). Several challenges were also identified and are being addressed.

***Action 12*: The Commission, in coordination with Member States, will work together with industry within the context of a contractual Public Private Partnership for cybersecurity, to develop and test technologies to better protect users and infrastructures against cyber aspects of hybrid threats.**

In July 2016 the Commission, in coordination with Member States, signed with industry a contractual Public Private Partnership (cPPP) for cybersecurity, investing up to €450 million under the EU research and innovation programme Horizon 2020, to develop and test technologies to better protect users and infrastructures against cyber and hybrid threats. The Partnership delivered the first pan-European Strategic Research Agenda, which focused on enhancing the resilience of critical infrastructure, as well as citizens against cyber-attacks. The Partnership increased coordination between

stakeholders, leading to efficiency and effectiveness gains in the cybersecurity funding under the Horizon 2020. The Partnership is working in parallel on issues related to Cybersecurity Certification of Information and Communications Technology as well as on how to tackle the acute shortage of cybersecurity skilled professionals in the market place. In view of the substantial needs for civil research and the high resilience required in defence, the European Defence Agency Cyber Research and Technology Group is contributing to the research areas identified by the European Cyber Security Organisation in their Strategic Research and Innovation Agenda.

Action 13: The Commission will issue guidance to smart grid asset owners to improve cybersecurity of their installations. In the context of the electricity market design initiative, the Commission will consider proposing 'risk preparedness plans' and procedural rules for sharing information and ensuring solidarity across Member States in times of crisis, including rules on how to prevent and mitigate cyber-attacks.

In the energy sector, the Commission is preparing a sectoral strategy on cybersecurity with the setting-up of the Energy Expert Cyber Security Platform to reinforce the implementation of the NIS Directive. A study in February 2017 identified Best Available Techniques to enhance the level of cyber-security of smart metering systems, supporting this platform. The Commission created also a web-based platform "*Incident and Threat Information Sharing EU Centre*", which analyses and shares information on cyber threats and incidents in the energy sector.

Enhancing financial sector's hybrid threat resilience

Action 14: The Commission, in cooperation with ENISA[15], Member States, relevant international, European and national authorities and financial institutions, will promote and facilitate threat information-sharing platforms and networks and address factors that hinder the exchange of such information.

Recognising that cyber threats are among the top risks to financial stability, the Commission reviewed the regulatory framework on payment services in the European Union, which is now subject to implementation. The revised Payment Services Directive[16] introduced new provisions to enhance security of payment instruments and strong customer authentication, with the aim of reducing fraud, especially in online payments. The new legislative framework will be applicable as of January 2018. Currently, the Commission, assisted by the European Banking Authority and in consultation with stakeholders, is developing regulatory technical standards, expected to be published by the end of 2017, on strong customer authentication and on common and secure communication to operationalise security in payment transactions. Furthermore, on the international front, the Commission has worked closely with the respective G7 partners on the "G7 fundamental principles of cyber security in the financial sector", endorsed in October 2016 by the G7 Finance Ministers and Central Bank's Governors. The principles are designed for financial sector entities (private and public) and contribute to a co-ordinated cybersecurity approach within the financial sector to jointly tackle cyber threats, including increased and more sophisticated cyber threats.

Transport

Action 15: The Commission and the High Representative (within their respective areas of competence), in coordination with Member States, will examine how to respond to hybrid threats, in particular those concerning cyber-attacks across the transport sector.

The implementation of the EU Maritime Security Strategy Action Plan[17] will help break the silos mentality in information exchange and shared use of assets between civilian and military authorities. A whole of government approach has led to increased cooperation across various actors. A joint Commission and EEAS civil-military Strategic Research Agenda is planned to be completed by the end of 2017, with a final workshop on protection of critical maritime infrastructure. This work could in the future expand to cover the emerging threat to sub-marine piping, energy transfer, fibre optic and traditional communications cabling from interference outside national waters.

A recent study[18] evaluated risk assessment capacity of national authorities carrying out coast guard functions. It identified the most important barriers to collaboration and recommended practical

ways to enhance cooperation between maritime authorities at EU and national level on this specific field. Risk assessment is essential in countering maritime threats and even more instrumental in the evaluation and prevention of hybrid threats, since they require additional and more complex considerations. The results of this study will be presented to different coast guard related fora so that the proposed recommendations can be assessed and implemented to increase cooperation in this field with preparedness and response to hybrid threats as the main objectives.

Countering terrorist financing

Action 16: The Commission will use the implementation of the Action Plan on Terrorist Financing to also contribute to countering hybrid threats.

Hybrid threats perpetrators and their supporters require funds to execute their plans. EU efforts against crime and terrorist financing under the European Agenda on Security and the Action Plan on terrorist financing can also contribute to countering hybrid threats. In December 2016, the Commission presented three legislative proposals, including on criminal sanctions of money laundering and illicit cash payments, as well as freezing and confiscation of assets[19].

All Member States needed to transpose by 26 June 2017 the 4th Anti-Money Laundering Directive[20], and in July 2016, the Commission submitted a targeted legislative proposal to complement and strengthen it with additional measures[21].

On 26 June 2017, the Commission issued the supranational risk assessment foreseen by the 4th Anti-Money Laundering Directive. It also put forward a proposal for a Regulation to prevent the importation and storage in the EU of cultural goods illicitly exported from third countries[22]. Later this year, the Commission will report on its ongoing assessment of the need for possible additional measures to track terrorist financing in the EU. The Commission is also reviewing legislation on combatting fraud and counterfeiting of non-cash means of payments.[23]

The Eighth report on progress towards an effective and genuine Security Union provides more details on the state of play of implementation of the Action Plan against Terrorist Financing.

Promoting EU common values and inclusive, open and resilient societies

Building resilience against radicalisation and violent extremism

Religious and ideological radicalisation, ethnic conflict and minority conflicts can be instigated by external actors through support to specific groups or through efforts to fuel conflicts among groups. Additional challenges have emerged, such as threats from lone actors, new pathways of radicalisation, including potentially in the context of the migratory crisis, as well as the rise of right wing extremism (including violence against migrants) and risks of polarisation. While work on radicalisation is taken forward within the Security Union context, it may be also indirectly relevant from the perspective of hybrid threats insofar as people vulnerable to radicalisation can be manipulated by hybrid threat perpetrators.

Action 17: The Commission is implementing the actions against radicalisation set out in the European Agenda on Security and is analysing the need to reinforce procedures for removing illegal content, calling on intermediaries' due diligence in managing networks and systems.

Preventing radicalisation

The Commission continues to implement its multi-faceted response to radicalisation as set out in the June 2016 Communication on supporting the prevention of radicalisation leading to violent extremism[24], with key actions such as promotion of inclusive education and common values, tackling extremist propaganda online and radicalisation in prisons, strengthening cooperation with third countries and enhancing research to better understand the evolving nature of radicalisation and better inform policy responses. The Radicalisation Awareness Network (RAN) has been at the forefront of the Commission's work to support Member States in this area, working with local practitioners at community level. More details are provided in the Eighth progress report towards an effective and genuine Security Union[25].

Online radicalisation and hate speech

In line with the European Agenda on Security[26], the Commission has taken steps to reduce the availability of illegal content online, notably through the EU Internet Referral Unit at Europol, and the EU Internet Forum[27]. Significant progress has also been made under the Code of Conduct countering illegal hate speech online[28]. More details are provided in the Eighth progress report towards an effective and genuine Security Union[29]. These actions will be reinforced, also in light of the European Council conclusions[30], the G7 Summit[31] and the Hamburg G20 Summit[32].

On-line platforms have a key role in tackling illegal or potentially harmful content. Under the Digital Single Market Strategy, as set out in the mid-term review[33], the Commission will ensure better coordination of platform dialogues focusing on the mechanisms and technical solutions for removal of illegal content. Where applicable, the aim should be to underpin these mechanisms with guidance on aspects, such as the notification and removal of illegal content. The Commission will also provide guidance on liability rules.

Increasing cooperation with third countries

Action 18: The High Representative, in coordination with the Commission, will launch a hybrid risk survey in neighbourhood regions. The High Representative, the Commission and Member States will use the instruments at their respective disposal to build partners' capacities and strengthen their resilience to hybrid threats. CSDP missions could be deployed, independently or to complement EU instruments, to assist partners in enhancing their capacities.

The European Union has increased its focus on building capacities and resilience in partner countries in the security sector, inter alia, by building on the nexus between security and development, developing the security dimension of the revised European Neighbourhood Policy and initiating counterterrorism and security dialogues with countries around the Mediterranean. To this extent a Pilot Project risk survey was launched with the cooperation of the Republic of Moldova. Its purpose is to help identify the country's key vulnerabilities and ensure that EU assistance targets specifically those areas. The results of the pilot showed that the survey in itself was deemed as useful. Building on the experience gained, the Commission and the EEAS will make recommendations to prioritise actions under the heading of building effectiveness, strategic communications, critical infrastructure protection and cyber security.

Looking ahead, additional neighbouring countries could benefit from the survey, building on this first experience; albeit with tailored adaptations to reflect the differing national local situations and specific threats and avoiding duplication with ongoing counterterrorism and security dialogues. More generally, on 7 June 2017 the Commission and the High Representative adopted a Joint Communication on "A Strategic Approach to Resilience in the EU's External Action"[34]. The aim is to support partner countries in becoming more resilient to today's global challenges. It recognises the need to move from crisis containment to a more structural, long-term approach to vulnerabilities, with an emphasis on anticipation, prevention and preparedness.

Cyber Resilience for Development

The EU is supporting countries beyond Europe in order to strengthen the resilience of their information networks. The ever increasing digitalisation has an intrinsic security dimension which brings particular challenges to the resilience of information networks systems globally as cyber-attacks know no borders. The EU supports third countries to build up their ability to adequately prevent and respond to accidental failures and cyber-attacks. Following a pilot cybersecurity project in the former Yugoslav Republic of Macedonia, Kosovo[35] and Moldova, concluded in 2016, the Commission will launch a new programme to enhance the cyber resilience of third countries, mainly in Africa and Asia for the period 2017-2020, but also in Ukraine. It aims to increase the security and preparedness of critical information infrastructure and networks in third countries on the basis of a whole-of-government approach, while ensuring compliance with human rights and rule of law.

Aviation Security

Civil aviation remains a major and symbolic target for terrorists but could also be targeted as part of a hybrid campaign. While the EU has developed a robust aviation security framework, flights originating from third countries may be more vulnerable. In line with UN Security Council resolution 2309 (2016), the Commission is stepping up efforts to build capacities in third countries. In January 2017, the Commission launched a new integrated risk assessment to ensure the prioritisation and coordination of capacity building efforts carried out at EU and Member State levels, as well as with international partners. In 2016, the Commission launched a 4-year project on Civil Aviation Security in Africa and the Arabian Peninsula to counter the threat of terrorism against civil aviation. The project focuses on sharing of expertise between partner States and experts from European Civil Aviation Conference Member States, mentoring, training and coaching activities. The activities will be further scaled up during 2017.

c. PREVENTING, RESPONDING TO CRISIS AND RECOVERING CRISES

While consequences can be mitigated through long term policies at national and EU level, in the short term it remains essential to strengthen the ability of Member States and the Union to prevent, respond and recover from hybrid threats in a swift and coordinated manner. A rapid response to events triggered by hybrid threats is essential. Much progress has been achieved in this area in the last year, with an operational protocol now in place in the EU laying out the crisis management process in the event of a hybrid attack. Regular monitoring and exercising will take place going forward.

Action 19: The High Representative and the Commission, in coordination with the Member States, will establish a common operational protocol and carry out regular exercises to improve strategic decision-making capacity in response to complex hybrid threats building on the Crisis Management and Integrated Political Crisis Response procedures.

The Joint Framework recommended the establishment of rapid response mechanisms to events triggered by hybrid threats, to coordinate among the EU response mechanisms[36] and early warning systems. To this end, the Commission services and the EEAS issued the EU operational protocol for countering hybrid threats (EU Playbook)[37], which outlines the modalities for coordination, intelligence fusion and analysis, informing policy-making processes, exercises and training, and cooperation with partner organisations, notably NATO, in the event of a hybrid threat. Similarly, NATO developed a playbook for enhanced NATO-EU interaction in preventing and countering hybrid threats in the areas of cyber defence, strategic communications, situational awareness and crisis management. The EU Playbook will be tested through an exercise in autumn 2017, as part of the European Union Parallel and Coordinated Exercise, which includes interaction with NATO.

Action 20: The Commission and the High Representative, in their respective areas of competence, will examine the applicability and practical implications of Articles 222 TFEU and Article 42(7) TEU in case a wide-ranging and serious hybrid attack occurs.

Article 42(7) TEU refers to armed aggression on a Member State's territory, while Article 222 TFEU (solidarity clause) refers to terrorist attack or natural or man-made disaster on a Member State's territory. The latter is more likely to be used in case of hybrid attacks, which are a mix of criminal/subversive actions. The invocation of the solidarity clause triggers coordination at Council level (Integrated Political Crisis Response arrangements, IPCR) and implication of relevant EU institutions, agencies and bodies, as well as EU assistance programs and mechanisms. Council Decision 2014/415/EU provides arrangements for the implementation by the Union of the solidarity clause. These modalities of application remain valid and there is no need to revise the Council decision. If a hybrid attack includes an armed aggression, Article 42(7) could also be invoked. In such a case, the aid and assistance shall be provided both by the Member States and by the EU. The Commission and the High Representative will continue to assess the most effective ways to address such attacks.

The adoption of the EU operational Protocol, mentioned above, directly supports this assessment and will be exercised as part of the EU Parallel and Coordinated Exercise (PACE) in October 2017. This exercise will test the EU's various mechanisms and ability to interact with the goal of speeding decision making where ambiguity triggered by a hybrid threat detracts from clarity.

<u>Action 21</u>: The High Representative, in coordination with Member States, will integrate, exploit and coordinate the capabilities of military action in countering hybrid threats within the Common Security and Defence Policy.

In response to tasking to Integrate Military Capabilities to support CFSP/CSDP, and following a seminar with Military Experts in December 2016, and guidance from the European Union Military Committee working group in May 2017, the military advice on "the EU military contribution to countering hybrid threats within the CSDP" was finalised in July 2017 and will be taken forward through the Concept Development Implementation Plan.

d. EU-NATO COOPERATION

<u>Action 22</u>: The High Representative, in coordination with the Commission, will continue informal dialogue and enhance cooperation and coordination with NATO on situational awareness, strategic communications, cybersecurity and "crisis prevention and response" to counter hybrid threats, respecting the principles of inclusiveness and autonomy of each organisation's decision making process.

On the basis of the Joint Declaration signed by the Presidents of the European Council and the European Commission, together with the Secretary General of NATO in Warsaw on 8 July 2016, the EU and NATO developed a common set of 42 proposals for implementation, which was subsequently endorsed in separate, parallel processes on 6 December 2016 by both the EU and NATO Councils[38]. In June 2017, the High Representative/Vice President and the Secretary General of NATO published a report on the overall progress made on the 42 actions of the Joint Declaration. Countering hybrid threats is one of the seven areas of cooperation identified in the Joint Declaration accounting for ten of the forty two actions. The report demonstrates that joint efforts undertaken over the past year have delivered substantial results. Many of the specific actions aimed at countering hybrid threats have already been mentioned, including the European Centre of Excellence for Countering Hybrid Threats, better situational awareness, establishment of the EU Hybrid Fusion Cell and its interaction with the newly created NATO Hybrid Analysis Branch and collaboration between strategic communications teams. For the first time, NATO and the EU staffs will exercise together their response to a hybrid scenario. This exercise is expected to test the implementation of over a third of the common proposals. The EU will carry out its own parallel and coordinated exercise this year and is preparing to take a leading role in 2018.

On resilience, both the EU and NATO staffs have engaged in cross-briefings, including on the EU mechanism for Integrated Political Crisis Response. Regular contacts between NATO and EU staffs, including through workshops and NATO or participation in the European Defence Agency's Steering Board, have allowed information exchanges on NATO’s baseline requirements for national resilience. Further exchanges between the Commission and NATO on bolstering resilience are planned for the autumn. The next progress report on EU-NATO cooperation will suggest possibilities for expanding cooperation between the two organisations.

3. CONCLUSION

The Joint Framework outlines actions designed to help counter hybrid threats and foster resilience at the EU and national level, as well as for partners. While the Commission and the High Representative are delivering in all areas in close cooperation with Member States and partners it is vital that this momentum is maintained in the face of ongoing and continuously evolving hybrid threats. Member States have the primary responsibility for countering hybrid threats related to national security and the maintenance of law and order. National resilience and collective efforts to protect against hybrid threats must be understood as mutually reinforcing elements of the same overall effort. Member States are therefore encouraged to carry out hybrid risk surveys as rapidly as possible as they will provide valuable information on the extent of vulnerability and preparedness across Europe. Building on the significant progress in improving awareness the potential of the EU Hybrid Fusion Cell should be maximised. The High Representative invites Member States to support the work of the StratCom Task Forces in order to counter more effectively the rise of hybrid threats. The EU will fully support the Finnish led European Centre for Countering Hybrid Threats.

The EU's unique strength lies in assisting Member States and partners to build their resilience, relying on a wide range of existing instruments and programmes. Significant progress has been made in actions to build resilience, in areas such as transport, energy, cybersecurity, critical infrastructure, protecting the financial system from illicit use and efforts to counter violent extremism and radicalisation. EU action in building resilience will continue, as the nature of hybrid threats evolves. In particular, the EU will develop indicators to improve protection and resilience of critical infrastructure against hybrid threats in relevant sectors.

The European Defence Fund may co-finance, together with Member States, capabilities priorities to strengthen resilience against hybrid threats. The upcoming Cybersecurity package, as well as cross-sectorial measures aimed at implementation of the Networks Information Security Directive, will provide for new platforms for countering hybrid threats across the EU.

The Commission and the High Representative call on Member States and stakeholders, where necessary, to reach swift agreement and to ensure rapid and effective implementation of the many measures aimed at bolstering resilience outlined in this Communication. The EU will build on and deepen its already fruitful cooperation with NATO.

The Union remains committed to mobilising all relevant EU instruments to address complex hybrid threats. Supporting Member States' efforts remains a priority for the Union, acting as a stronger and more responsive security provider, alongside its core partners.

Notes:

1. Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", JOIN (2016) 18 final.

2. *Council conclusions on countering hybrid threats*, Press Release 196/16, 19 April 2016.

3. Presented by the High Representative to the European Council on 28 June 2016.

4. COM(2016) 230 final, 20.4.2016.

5. The Bratislava Roadmap of the European Council from 16 September 2016 and The Rome Declaration of the leaders of 27 member states and of the European Council, the European Parliament and the European Commission from 25 March 2017.

6. http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-conclusions-eu-nato-cooperation

7. Reflection paper on the future of European defence, 7.6.2017, https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_en.pdf

8. To date, 21 Member States have nominated national points of contact. These are individuals working in Member States capitals in a policy / resilience role.

9. Finland, France, Germany, Latvia, Lithuania, Poland, Sweden, United Kingdom, Estonia, Spain.

10. The Centre is open for other EU Members States and NATO Allies to join.

11. https://www.easa.europa.eu/system/files/dfu/208599_EASA_CONFLICT_ZONE_CHAIRMAN_REPORT_no_B_update.pdf

12. https://ad.easa.europa.eu/czib-docs/page-1

13. European Council conclusions of 22-23 June 2017.

14. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p.1.

15. European Union Network and Information Security Agency.

16. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, OJ L 337, 23.12.2015, p. 35.

17. https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf and the 2nd report on the implementation of the EUMSS AP presented to Member States on 21 June 2017.

18. Study on "Evaluation of risk assessment capacity at the level of Member States' authorities performing coast guard functions", https://ec.europa.eu/maritimeaffairs/documentation/studies; https://bookshop.europa.eu/en/evaluation-of-risk-assessment-capacity-at-the-level-of-member-states-authorities-performing-coast-guard-functions-in-order-to-identify-commonalities-and-ways-to-enhance-interoperability-and-cooperation-in-this-field-across-eu-pbEA0417344/?CatalogCategoryID=JRWep2OwmH0AAAFEQf8mwjCM.

19. Third progress report towards an effective and genuine Security Union (COM(2016) 831 final).

20. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance), OJ L 141, 5.6.2015, p. 73–117.

21. For more details please see the Third progress report towards an effective and genuine Security Union (COM(2016) 831 final) and the Eighth progress report towards an effective and genuine Security Union (COM(2017) 354 final).

22. COM(2017) 26.6.2017, COM(2017) 340 final, SWD(2017) 275 final.

23. Eighth progress report towards an effective and genuine Security Union (COM(2017) 354 final).

24. http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf

25. COM(2017) 354 final.

26. For more details please see the Eighth progress report towards an effective and genuine Security Union COM(2017) 354 final.

27. For more details please see the Eighth progress report towards an effective and genuine Security Union COM(2017) 354 final.

28. Code of Conduct on illegal online hate speech, 31 May 2016, http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf

29. For more details please see the Eighth progress report towards an effective and genuine Security Union COM(2017) 354 final.

30. Council Conclusions 22-23 June 2017.

31. G7 summit in Taormina, Italy, 26-27/05/2017.

32. G20 summit in Hamburg, Germany, 07-08/07/2017.

33. Cf. above Communication from the Commission COM(2017) 228 final.

34. Joint Communication to the European Parliament and the Council: “A Strategic Approach to Resilience in the EU's external action”, JOIN (2017) 21 final.

35. This designation is without prejudice to positions on status, and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.

36. The Council's EU Integrated Political Crisis Response (IPCR) arrangements, the Commission's ARGUS system and the EEAS' CRM.

37. Staff Working Document (2016) 227 adopted 7 July 2016.

38. http://www.consilium.europa.eu/en/press/press-releases/2016/12/06-eu-nato-joint-declaration/

Elements of Bibliography

The bibliography is incorporated in the footnotes. The publications quoted hereunder have been particularly useful for the author to complete her study.

Reference works

- J. Henrotin, *Techno-guérilla et guerre hybride. Le pire des deux mondes*, Paris, 2014.
- Revue Défense Nationale, *Penser la guerre… hybride ?*, March 2016.
- Stratégique No 111, *Hybridité et Guerre hybride*, May 2016.

NATO documents

- SHAPE (Supreme Headquarters Allied Powers Europe) and SACT (Supreme Allied Commander Transformation) joint communication, *BI-SC Input to a new NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats*, 25 August 2010 (http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf).
- NATO Press Release, *Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*, 5 September 2014, (https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en).
- NATO Press Release, *Press Conference by NATO Secretary General Jens Stoltenberg Following the Meeting of the North Atlantic Council at the Level of Defence Ministers*, 11 February 2016 (https://www.nato.int/cps/en/natohq/opinions_127972.htm?selectedLocale=en)
- NATO Press Release, *Warsaw Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016* (https://www.nato.int/cps/en/natohq/official_texts_133169.htm).

EU documents

- European Defence Agency, *Hybrid Warfare threats – Implications for European capability development. Strategic context report: relevance of hybrid threats for European security*, 30 November 2015 [SCS/P003198].

- EU Military Staff, *Draft Food for Thought Paper: Possible EU Military Contributions to Countering Hybrid Threats*, 2 October 2015 [EEAS (2015) 1367 REV1].
- European Commission, Joint Communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats: a European Union response", 6 April 2016 [JOIN (2016) 18 final] (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en).
- European Parliament, *Countering hybrid threats: EU-NATO cooperation*, March 2017 (http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf).
- European Council, Presidency Note: *Mandate of the Friends of the Presidency Group on the Implementation of Action 1 of the Joint Framework on Countering Hybrid Threats (doc. 7688/16)*, 2 June 2017 [9502/17].
- European Commission, Joint Report to the European Parliament and the Council on the implementation of the "Joint Framework on countering hybrid threats: a European Union response", Brussels, 19 July 2017 [JOIN (2017) 30 final] (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0030&from=EN).

Royal Higher Institute for Defence
Centre for Security and Defence Studies
30 avenue de la Renaissance
1000 Brussels