Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 14523
06 April 2018

Legal challenges related to hybrid war and human rights obligations

Report[1]
Committee on Legal Affairs and Human Rights
Rapporteur: Mr Boriss CILEVIČS, Latvia, Socialists, Democrats and Greens Group

Summary

States are more and more often confronted with the phenomenon of "hybrid war", which covers not only military actions, but also other hostile acts, such as disinformation campaigns via social media and cyberattacks.

The concept of "hybrid war" or "hybrid threat" raises several questions. The Committee on Legal Affairs and Human Rights considers that although there is no universal definition for these terms, the main feature of a "hybrid war" is its "legal asymmetry", as hybrid adversaries deny their activities and operate on the very fringes of the law. While military actions are underway, international law, especially the right to self-defence and humanitarian law, apply. In the event of non-military actions, it is above all domestic criminal law that comes into play. In all cases, human rights must be respected. Any restriction of these rights must comply with the requirements resulting from the European Convention on Human Rights.

The committee also proposes a number of recommendations to be addressed to member States and to the Committee of Ministers in order to combat "hybrid war" more effectively and to uphold human rights in the fight against this phenomenon.

1. Reference to committee: Doc. 14044 and Doc. 14048, Reference 4217 of 20 June 2016.

Contents **Page**

A. Draft resolution[2]

1. The Parliamentary Assembly recalls its Resolution 2133 (2016) on legal remedies to human rights violations on the Ukrainian territories outside the control of the Ukrainian authorities and Resolution 2132 (2016) on the political consequences of the conflict in Ukraine and its Resolution 2198 (2018) and Recommendation 2119 (2018) on the humanitarian consequences of the war in Ukraine concerning the military operations in Ukraine. It also recalls its Resolution 2190 (2016) on prosecuting and punishing the crimes against humanity or even possible genocide committed by Daesh.

2. The Assembly notes with concern that today States are more and more often confronted with the phenomenon of "hybrid war", which poses a new type of threat based on a combination of military and non-military means such as cyberattacks, mass disinformation campaigns, including fake news, in particular via social media, disruption of communications and other networks and many others. Cyberattacks are particularly dangerous as they can hit a country's strategic infrastructure, such as its air traffic control system or nuclear plants. Therefore, hybrid war can destabilise and undermine entire societies and cause numerous casualties. The increasingly widespread use of these new tactics, especially in combination, raises concerns about the adequacy of existing legal norms.

3. The Assembly notes that there is no universally agreed definition of "hybrid war" and there is no "law of hybrid war". However, it is commonly agreed that the main feature of this phenomenon is "legal asymmetry", as hybrid adversaries, as a rule, deny their responsibility for hybrid operations and try to escape the legal consequences of their actions. They exploit lacunas in the law and legal complexity, operate across legal boundaries and in under-regulated spaces, exploit legal thresholds, are prepared to commit substantial violations of the law and generate confusion and ambiguity to mask their actions.

4. Despite the complexity of hybrid war, the Assembly stresses that hybrid adversaries do not operate in a legal vacuum and that relevant domestic and international law norms, including international human rights law, apply to their actions, although the question of attribution and hence accountability may raise difficulties. If, in the framework of hybrid war, a State resorts to the use of force against another State, the latter State is allowed to invoke the right to self-defence on the basis of Article 51 of the Charter of the United Nations and norms of international humanitarian law will apply. However, in practice, hybrid adversaries avoid manifest use of force that would reach the required threshold for triggering application of the above norms, thereby creating a legal grey area.

5. The Assembly notes that in cases in which a hybrid adversary refrains from the use of military means, its actions should be examined in the light of domestic criminal law and, if necessary and depending on the situation, relevant international legal instruments covering specific policy areas (such as the law of the sea or norms on combating cybercrime, terrorism, hate speech or money laundering).

6. The Assembly recalls that when countering hybrid war, States are bound to respect human rights law. It is concerned that certain member States of the Council of Europe have already taken measures (such as criminal convictions for online statements, surveillance measures, blocking websites or expulsions) which raise questions concerning respect for human rights, such as the right to freedom of expression, including the right to information, the right to respect for one's privacy or freedom of movement.

7. The Assembly also recalls that although Article 15 of the European Convention on Human Rights (ETS No. 5, "the Convention") allows States Parties to derogate from certain obligations "in time of war or other public emergency threatening the life of the nation", any derogation from the rights enshrined therein shall be made according to certain substantive and procedural requirements. When countering hybrid war threats, States Parties to the Convention may also invoke "national security" as a "legitimate aim" to limit certain rights: the right to respect for private and family life (Article 8), freedom of expression (Article 10), freedom of assembly and association (Article 11), freedom of movement (Article 2.3 of Protocol No. 4 to the Convention (ETS No. 46)) and procedural safeguards in case of the expulsion of aliens (Article 1.2 of Protocol No. 7 to the Convention (ETS No. 117)). Any restriction of the above rights shall be "prescribed by law", "necessary in a democratic society" and proportionate. Experience gained by States in counterterrorism activity may be a useful source of guidance when identifying the limitations imposed by international law on measures to counter hybrid war threats.

2. Draft resolution adopted unanimously by the committee on 14 March 2018.

8. Therefore, the Assembly calls on member States to:

8.1. refrain from resorting to hybrid war in international relations and fully respect the provisions of international law, in accordance with their object and purpose, by not abusively exploiting perceived loopholes or ambiguities;

8.2. step up international co-operation in order to identify hybrid war adversaries and all types of hybrid war threats, as well as to establish the applicable legal framework;

8.3. take measures to increase the public's awareness of hybrid war threats and its ability to react speedily to such threats;

8.4. implement the Council of Europe Convention on Cybercrime (ETS No. 185), sign and ratify it where this is not already the case, and promote its ratification by non-member States.

9. The Assembly welcomes the measures taken by the European Union and the North Atlantic Treaty Organization (NATO) to counter hybrid war threats and to establish co-operation in this field. It also calls on all Council of Europe member States which are members of the European Union and NATO to share their best practices on countering hybrid war with other member States that may be affected by this phenomenon.

10. As regards measures aimed at countering hybrid war, the Assembly recalls its Resolution 1840 (2011) on human rights and the fight against terrorism. It calls on member States to ensure that such measures respect the requirements stemming from the European Convention on Human Rights, in line with interpretation given by the European Court of Human Rights. In particular, as regards rights that are subject to restrictions under the Convention, any limitation must be based on law, proportionate to the legitimate aim pursued (for example national security) and "necessary in a democratic society".

B. Draft recommendation[3]

1. The Parliamentary Assembly refers to its Resolution … (2018) on legal challenges related to hybrid war and human rights obligations.

2. The Assembly recommends that the Committee of Ministers:

2.1. conduct a study on hybrid war threats, with a special focus on non-military means, in order to identify legal gaps and develop appropriate legal standards, including considering a new Council of Europe convention on this subject;

2.2. develop principles for regulatory reform of social media platforms to ensure transparency in the conduct of free and fair elections;

2.3. examine State practice in countering hybrid war threats, with a view to identifying legal standards and good practice and ensuring compliance of this practice with the safeguards provided for by the European Convention on Human Rights (ETS No. 5);

2.4. step up co-operation with other international organisations working in this field, in particular the European Union and the North Atlantic Treaty Organisation (NATO);

2.5. promote the ratification by member and non-member States of the Convention on Cybercrime (ETS No. 185);

2.6. examine ways in which the Convention on Cybercrime is implemented by its States Parties and initiate a reflection on whether it could be improved.

3. Draft recommendation adopted unanimously by the committee on 14 March 2018.

C. Explanatory memorandum by Mr Boriss Cilevičs, rapporteur

1. Introduction

1.1. Procedure

1. On 20 June 2016, the Parliamentary Assembly referred two motions for a resolution, entitled "Restricting rights to protect national security – how far can States go" and "Legal challenges arising from the hybrid war", to the Committee on Legal Affairs and Human Rights, to be merged into a single report.[4] At its meeting in Strasbourg on 10 October 2016, the committee appointed me as rapporteur. At its meeting in Paris on 13 November 2017, the committee held a hearing with the participation of Mr Andrey L. Kozik, Associate Professor, Secretary-General of the International Law and Arbitration Association, Belarus, Mr Robin Geiß, Professor, Chair of International Law and Security, University of Glasgow School of Law, United Kingdom, and Dr Aurel Sari, Senior Lecturer in Law, Director of the Exeter Centre for International Law, University of Exeter Law School (United Kingdom).

1.2. Issues at stake

2. When preparing this report, I have to take into account various issues raised in the two motions. The motion on "Restricting rights to protect national security – how far can States go?" notes that attempts to limit fundamental freedoms are now being made under the pretext of having to defend against an undeclared hybrid war, a concept that is not legally defined. In this context, some member States of the Council of Europe are criminalising the expression of certain opinions considered to constitute a threat against the State. The signatories of this motion recall that defending the constitutional order and national security may be legitimate aims justifying limitations on certain human rights and fundamental freedoms, provided such limitations are compatible with the requirements of the European Convention on Human Rights (ETS No. 5, "the Convention"), as interpreted by the European Court of Human Rights ("the Court"). The Assembly should examine these issues in the light of Council of Europe standards to analyse whether such restrictions can be justified and, if so, on what conditions.

3. The second motion focuses on the concept of hybrid war, which is often used in relation to, for example, the ongoing military conflict in Ukraine and the activities of Daesh. According to the motion, hybrid war poses a new type of threat based on a combination of military and non-military means such as cyberattacks, mass disinformation campaigns via social media, disruption of communications and many others. The widespread use of these new tactics, especially in combination, raises concerns about the adequacy of existing norms. The Assembly should therefore identify legal gaps and subsequently draw up appropriate standards which would enable defensive measures to be taken even in the absence of a direct armed attack by another State. Such measures would also create safeguards against the selective application of international law.

4. Bearing in mind the content of the two motions, I feel obliged, as rapporteur, to examine at the same time two – both contradictory and complementary – proposals: on one hand, how to define "hybrid war"/ "hybrid warfare" or "hybrid war threats" and identify the measures that a State may properly take to defend itself against such actions, in compliance with international law; and on the other, how to protect human rights and fundamental freedoms when a State seeks to limit them with the aim of defending itself against a range of hybrid war measures used against it by another State or a powerful non-State actor such as Daesh. As regards the latter issue, I would like to recall that the Assembly has already considered the problem of restrictions on human rights and fundamental freedoms imposed in the interests of national security and public safety in the context of the fight against terrorism (see, in particular, reports and resolutions on "Human rights and the fight against terrorism" and "National security and access to information"[5]). The Assembly has on many occasions reiterated that terrorism can and must be effectively combated by means that fully respect human rights and the rule of law.[6]

---

4. Doc. 14044 and Doc. 14048.
5. See, respectively, Assembly reports Doc. 12712 of 16 September 2011 (rapporteur: Lord John Tomlinson) and Doc. 13293 of 3 September 2013 (rapporteur: Mr Arcadio Díaz Tejera), as well as the Assembly Resolution 1840 (2011), Resolution 1954 (2013) and Recommendation 2024 (2013).
6. For example, in Resolution 1840 (2011), paragraphs 5-7.

1.3. Hybrid threats: a growing phenomenon

5. In recent years, "hybrid (war) threats" have become one of the top security concerns in Council of Europe member States. On the one hand, United States and European security experts often refer to the growing Russian multilevel threat to security, giving the example of the Russian hybrid operations in eastern Ukraine, Crimea or Georgia.[7] In 2016, issues related to this conflict were examined by our committee in the report by Ms Marieluise Beck (Germany, ALDE) on "Legal remedies to human rights violations on the Ukrainian territories outside the control of the Ukrainian authorities", by the Committee on Political Affairs and Democracy in the report by Ms Kristýna Zelienková (Czech Republic, ALDE) on "Political consequences of the conflict in Ukraine" and by the Committee on Migration, Refugees and Displaced Persons in the report by Mr Egidijus Vareikis (Lithuania, EPP/CD) on "Humanitarian consequences of the war in Ukraine".[8] On the other hand, the concept is also used by Russian strategists to designate Western countries' efforts to undermine "unfriendly governments".[9] For example, Russian officials draw a direct parallel between hybrid war and an attempt to damage the government's integrity in the context of the so-called "colour revolutions", which occurred in former Soviet republics such as Georgia, in 2003, or Ukraine, in 2004. The Russian Defence Minister, Sergei Shoigu, stated that "Colour revolutions are increasingly taking on the form of warfare and are developed according to the rule of war craft".[10]

6. It should be noted that the use of non-military means of warfare are neither new (according to some scholars, "hybridity" dates back to the Peloponnesian War[11]) nor specific to any country.[12] With technological advances, however, come new means of soft power and warfare. "Hybrid war threats" focus on the exploitation of a country's vulnerabilities, often with the aim of undermining its essential features (i.e. political regime and ideology, economy, territorial integrity). This is particularly relevant in the area of cybersecurity. Today, our extensive reliance on computer systems and digital networks has completely reshaped the way in which energy, finance, telecommunication and transportation systems – i.e. all that constitutes the State's critical infrastructure – are conceived and operate. It has also changed the way in which democracy and fundamental rights are protected, particularly freedom of expression and access to information. Some recent phenomena such as "information warfare" (which is not new as such but has reached critical size) and "cyberattacks", which are not geographically limited, illustrate very well these new challenges.

7. "Information warfare", which is defined by some scholars as the "conflict or struggle between two or more groups in the information environment",[13] aims to impose a specific viewpoint on a population by "creating [an] impenetrable, active and offensive information dominance".[14] The aim of an "information war" is to win over the population.[15] In essence, information warfare combines electronic warfare (including electronic counter measures and jamming), cyberwarfare (which will be analysed in detail below) and psychological operations ("psy-ops", which are aimed at degrading the morale and well-being of a nation's citizens, for example by spreading false information through social media and news outlets). Such campaigns seem to be most successful in regions that are already unstable. Russian disinformation campaigns, for instance, fell on fertile ground in Crimea and the Donbas region, where a part of the population was already inclined to accept the Russian narrative of events.[16] In its report "on the political consequences of the conflict in Ukraine", the Committee on Political Affairs and Democracy described Russia's involvement with extensive information operations and its propaganda war as just "as dangerous as the military one".[17] Therefore, States with minority ethnic Russian populations are understandably concerned about such a threat. However, the United States and some other European countries are also exposed to this phenomenon. Although systematic influencing of public opinion and electoral processes is not new *per se*, its scale has considerably increased in

---

7. NATO, Hybrid war – Does it even exist?, NATO review, 2015, and Keynote speech by NATO Secretary General Jens Stoltenberg at the opening of the NATO Transformation Seminar, 25 March 2015; see also John Swaine, "Georgia: Russia 'conducting cyber war'", *The Telegraph*, 11 August 2008.
8. See, respectively, Doc. 14139 of 26 September 2016 and Assembly Resolution 2133 (2016); Doc. 14130 and the Resolution 2132 (2016) , as well as Doc. 14463 and Resolution 2198 (2018) and Recommendation 2119 (2018).
9. Samuel Charap, The Ghost of Hybrid Warfare, *Survival, Global Politics and Strategy,* Issue 57/6, 51-56.
10. Alexander Golts, Are Colour Revolutions a New Form of War?, *The Moscow Times*, 2 June 2014.
11. A. Sari, Hybrid Warfare, Law and the Fulda Gap, University of Exeter, Law School, 2017, p. 9.
12. B. Renz and H. Smith, *et al*., Russia and Hybrid Warfare, Going Beyond the Label, *Aleksanteri Papers 2016/1*, Kikimora Publications, University of Helsinki, 2016, p. 11.
13. I. Porche III and others, Redefining Information Warfare Boundaries for an Army in a Wireless World, RAND Corporation, 2013, p. XV.
14. Christian Bahnareanu, The evolution of warfare from classic to hybrid actions, *Strategic Impact*, Issue 2/2015, pp. 61-62.
15. B. Renz and H. Smith, *supra* note 12, p. 6.
16. David Stupples, What is information warfare?
17. See paragraph 84 of the report.

recent years. The example of the United States, where 126 million citizens were allegedly exposed to Russian misinformation before the latest presidential election in 2016, is a particularly striking example.[18] Moreover, similar interferences in the electoral process have apparently occurred in Germany, France and some countries in the Balkan region.

8. In information warfare, the lack of accountability and attribution online make it difficult for States to determine what falls within the realm of freedom of expression and what qualifies as foreign interference. This is particularly difficult when foreign financing is involved. *Sputnik news* and *RT* (formerly *Russia Today*), for example, have European branches and are financed by Russian assets, while the US right-wing *Breitbart News* has opened offices in Europe. In the current debate over how online "fake news" shapes public opinion, inquiries into the connection between foreign powers and such news outlets are important. Even without a physical presence in a particular country, sources of misinformation can nevertheless penetrate the information environment and influence public discourse, especially where internet access and content is free and regulated on narrow grounds. "Online trolls" also fall into a grey area between individuals expressing their opinions and semi-organised non-State actors following a particular State's political agenda. The example of Russian "troll factories"[19] makes it increasingly difficult to distinguish the line between online activists' free speech and State interference. Moreover, the broadcasting of audiovisual programmes across States' borders raises questions as the control and jurisdiction over the content broadcast to States in which the broadcaster is not established (e.g. a Russian broadcaster established in Sweden broadcasting to the Baltic States), which might require a revision of the EU Audiovisual Media Service Directive (2010/13/EU) and the Council of Europe European Convention on Transfrontier Television (ETS No. 132).

9. "Cyberwarfare"/"cyberattack", is a particularly violent and dangerous form of "hybrid threat", as it may hit strategic infrastructure such as air traffic control systems, oil pipeline flow systems or nuclear plants. In the past ten years, several countries, including former Soviet republics (Estonia, Georgia, Lithuania and Ukraine) or western countries (Finland, Germany, the Netherlands and the United States) claim to have been exposed to Russian cyberattacks. There have also been a number of high-profile strategic multi-level interferences, including in presidential elections in the United States in 2016 and in Ukraine in 2014. In France, in May 2017, tens of thousands of emails and documents from Emmanuel Macron's campaign were released immediately prior to the second round of the presidential election.

10. States have already taken measures to protect themselves from perceived hybrid terrorist threats. Some European countries have passed counterterrorism laws that may be used against such threats, but some of these measures might violate human rights (as denounced by Amnesty International).[20] Cyberwarfare may lead States to restrict citizens' internet freedom by developing "filtering techniques" in order to limit access to certain sites and surveillance mechanisms in order to monitor citizens' use of internet, and by instituting criminal proceedings against individuals for online actions. States' responses to Russian misinformation campaigns already affect their citizens. For example, in Latvia, Maksim Koptelov was sentenced to six months in prison for a peaceful online petition proposing that Latvia join Russia. A few days later, police investigated another Latvian citizen, Deniss Barteckis after he posted a similar online petition calling for Latvia to join the United States. While it is normal for States to criminalise acts that threaten their independence and territorial integrity, in these cases the punishment appears to be a disproportionate response to a peaceful political expression. Other States have also taken controversial measures to counter hybrid threats. For example, in May 2017, Ukraine's President Petro Poroshenko signed a decree blocking access to numerous Russian websites (including social networks). In Germany, in June 2017, the *Bundestag* passed the Act to Improve Enforcement of the Law in Social Networks, which enables authorities to issue fines of up to 50 million euros against social media companies which fail to remove hate speech, incitements to violence and defamation within 24 hours. In France, in January 2018, President Macron announced that a special law was needed to combat "fake news". All those measures may raise questions as to their compatibility with freedom of expression.

---

18. These data come from Facebook, Twitter and Google representatives giving evidence at a hearing at the US Congress on 31 October 2017. See, for instance, Russia used mainstream media to manipulate American voters, *Washington Post*, 15 February 2018.

19. Mike Wendling and Will Yates, "NATO says viral news outlet is part of 'Kremlin misinformation machine", BBC, 11 February 2017; Emily Flitter, "Riding Trump wave, Breitbart News plans U.S., European Expansion", Reuters, 9 November 2016, and Andrew Higgins, "Effort to Expose Russia's 'Troll Army' Draws vicious Retaliation", *New York Times*, 30 May 2016.

20. Amnesty international, "Dangerously Disproportionate, the Ever-Expanding National Security State in Europe", Report, January 2017.

11. States are thus now facing complex multi-level security threats and have accordingly taken steps to tackle their vulnerabilities to them. As this is a relatively recent trend in terms of both international and national security, the concept of "hybrid (war) threat" remains a rather ambiguous one. Thus, the first aim of my report would be to examine the different concepts and the legal challenges stemming from them, and particular to reflect on whether "hybrid war" is a "war" within the meaning of international humanitarian law. Moreover, since "hybrid threats" are already considered in States' national security strategies, it is possible to review certain measures taken to counter these threats posed by State and/or non-State actors. National security is considered a legitimate aim permitting interference with human rights under the Convention, on certain conditions. Although States have traditionally been allowed a relatively wide discretion when evaluating security threats and deciding on the measures to be taken in response, those measures must nevertheless respect human rights law. In relation to measures taken to protect national security against hybrid threats, the legal limits imposed on States regarding human rights and fundamental freedoms should therefore also be examined.

2. Legal challenges related to hybrid threats

2.1. Definitions

12. According to the European Parliament Research Service (EPRS),[21] a "hybrid threat" is "a phenomenon resulting from convergence and interconnection of different elements, which together form a more complex and multidimensional threat". Taking into account different levels of intensity of a threat and intentionality of actors involved, the EPRS also defines a "hybrid conflict" and a "hybrid war". A "hybrid conflict" is "a situation in which parties refrain from the overt use of armed forces against each other, relying instead on a combination of military intimidation (falling short of an attack), exploitation of economic and political vulnerabilities, and diplomatic or technological means to pursue their objectives". Finally, "hybrid war" is "a situation in which a country resorts to overt use of armed forces against another country or a non-State actor, in addition to a mix of other means (i.e. economic, political, and diplomatic)".

13. In the context of States' national security protection practices and their legal limits, it is more accurate to use the terms "hybrid threat" or "hybrid conflict". "While the 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 co-ordinated manner by State or non-State actors to achieve specific objectives while remaining below the threshold of formally declared warfare."[22] Indeed, "hybrid threat" is often seen as a "catch all" notion, used to designate the occurrence of simultaneous security threats. According to the EPRS, it may cover various situations, including terrorist acts (of Boko Haram, Al-Queda or Daesh), actions against cybersecurity (see below), actions of armed criminal groups (such as those of Mexican drug cartels), maritime disputes (in the South China Sea), constraints on the use of orbital space, hostile economic acts (such as the blocking of Japanese exports by China in 2010) or covert military operations (like the use of "green men" in Crimea). "Hybrid threats" may emanate both from States and non-State actors and they can cover both violent and non-violent forms of confrontation; the European Union has given preference to this term due to the scope of its mandate and has mainly focused on "security threats". However, the term "hybrid war", which focuses attention on violent activities, should not pose any problem to NATO.[23]

14. Legally speaking, it is more precise to use the term "hybrid war" only when an armed conflict exists, and therefore the application of international humanitarian law is triggered. International relations and conflict analysis scholars perceive "hybrid war" as the combination of security threats which were previously considered separately. The concept of "hybrid war" combines conventional kinetic capabilities with irregular tactics and formations such as terrorism, transnational crimes and weapons proliferation, especially when committed by actors apparently associated with a particular State but officially not under its authority. Other non-kinetic and low intensity means can also fall under this definition, such as cyberoperations and disinformation and propaganda, targeting also relevant national or other minorities, and corruption of key

21. At a glance. Understanding hybrid Threats, European Parliament Research Service (EPRS), June 2015.
22. European Commission, "Joint communication to the European Parliament and the Council, Joint framework on countering hybrid threats, a European Union response", Brussels, 6 April 2016, JOIN(2016) 18 final, paragraph 1.
23. A. Sari, *supra* note 11, p. 15. Nevertheless the term of hybrid "threats" is also widely used, officially, by NATO and its related researches. See NATO Countering the hybrid threat, NATO website, or Guillaume Lasconjarias and Jeffrey A. Larsen, *NATO's Response to Hybrid-Threats*, NATO Defence College, NDC Forum Papers Series, Rome, 2015.

actors through the use of "black funds" or "parallel budgets".[24] Hybrid war refers to both State and non-State actors' activities. These activities are considered to be directed and co-ordinated with the aim of achieving a "synergistic effect in the physical and psychological dimensions of conflict".[25]

15. Numerous scholars see this type of threat as inherently new. The proliferation of hybrid warfare has been encouraged by "the emergence of new sub-State players, new types of weapons and new ideological representation".[26] Other researchers consider that hybrid war is nothing more than a label and that those characteristics presented as new could already be seen in the past in the practices of State and non-State actors. Moreover, those scholars consider that the term "war" is misleading in this context. Despite this, it is generally agreed that in addition to classic warfare actions, there is nowadays a pre-eminent occurrence of asymmetrical, unconventional and hybrid actions, often waged by non-State actors.[27] As stressed by the experts who took part in the hearing before the committee in November 2017, "hybrid war" or "hybrid warfare" is a political concept rather than a legal one and asymmetry is its main feature. As underlined by Mr Robin Geiß, although there are many definitions of "hybrid war", the essence of each of them is the recourse to "unexpected and unorthodox use of subversive tactics". As stressed by Mr Aurel Sari, the definition of "hybrid warfare threats" included in NATO's Wales Summit Declaration of September 2014 rightly put emphasis on "a highly integrated design", in which "a wide range of overt and covert military, paramilitary, and civilian measures" were employed. This expert focuses on the notion of "hybrid adversary" that aims to create such an asymmetry by exploiting legal thresholds, complexity and uncertainty; generating legal ambiguity; violating its legal obligations and utilising law to support its strategic narrative and counter-narrative. All this is being done to create a legal environment that favours its own operations and disadvantages the operations of its target. This definition puts emphasis on the use of law as an instrument of warfare and on both its defensive and offensive aspects.

16. Interestingly, according to Mr Sari, excluding the use of armed force from the definition of "hybrid threats" "reduces hybridity to a loose synonym of complexity". The concept of "hybrid threats" should be reserved for situations where States or non-State actors employ non-violent means of warfare as instruments of warfare by integrating them with the use of armed force or the threat of force. Scholars have not shown much interest in the legal aspects of "hybrid warfare", as most of the legal problems related to this concept – such as violation of territorial integrity, support for separatist movements or the failure to honour international agreements – are not new. The breadth and fluidity of this concept make it difficult for it to be legally assessed.[28]

17. Therefore, despite the fact that "hybrid threats" are described as a "catch all" concept, there is no universally agreed definition of the concept, and some conceptual differences can be seen. According to Mr Geiß, there is no need to define "hybrid war", as the existing definition of "war" is sufficient, but, there is a need to specify hybrid threats. Legally, the term "hybrid war(-fare)", which is a political one, describes the existence of an armed conflict in which conventional military techniques (but not only) are used. I will use this term in this meaning. As regards the other terms – "hybrid threats" or "hybrid conflicts" – they are used in relation to other – non-military – "hybrid" means of conflict. Referring to this definition, I will only use the term "hybrid threats".

2.2. Applicable legal framework

2.2.1. Hybrid war

18. In international law, the use of force by States is regulated by *jus ad bellum.* Article 2 of the Charter of the United Nations prohibits the threat or use of force "against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations" (paragraph 4) and reaffirms the principle of non-intervention in matters which are essentially within the domestic jurisdiction of any State (paragraph 7). Article 51 of the Charter provides for an exception to the rule included in Article 2.4: States have the right of individual or collective self-defence if an armed attack occurs.[29] UN General

24. See the report by Mr Andreas Gross (Switzerland, SOC) on "Refusing impunity for the killers of Sergey Magnitsky", Doc. 13356, paragraph 171.
25. Frank G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Warfare, Potomac Institute for Policy Studies, Arlington, Virginia, December 2007, p. 8.
26. François-Bernard Huyghe, The impurity of war, *International Review of the Red Cross,* Vol. 91/873, March 2009.
27. See B. Renz and H. Smith et al., *supra* note 12, and Christian Bahnareanu, *supra* note 14, pp. 57-66.
28. A. Sari, *supra* note 11, pp. 16 and 18.
29. The second exception is included in Article 42 of the UN Charter, which authorises the Security Council to take military measures to maintain or restore international peace and security.

Assembly Resolution 2625 of 25 October 1970 reaffirms the prohibition of the threat or use of force and the principle of non-intervention. It also stresses that "States have the duty to refrain from propaganda for wars of aggression".

19. The right of self-defence, which is well established in customary international law, is triggered by an armed attack. If the intensity of a hybrid adversary's operations does not reach the necessary level or limits itself to the threat of force, the right to respond by using force in self-defence cannot be invoked. In the case Nicaragua v. United States, the International Court of Justice (ICJ) reaffirmed that the right of self-defence can only be exercised in response to an "armed attack" (which was interpreted in the light of the Article 3(g) of the Definition of Aggression annexed to the UN General Assembly Resolution 3314 (XXIX) of 1974). The ICJ found, *inter alia*, that assistance to rebels in the form of the provision of weapons or logistical or other support did not fall within the scope of this right; however, "such assistance may be regarded as a threat of use of force, or amount to intervention in the internal or external affairs of other States".[30] This leaves a legal gap between the use of force and an armed attack: a gap that is not recognised by the United States, which takes the position that any use of force gives rise to, in principle, the right of self-defence. Therefore, while combating terrorism, the United States excessively expanded the concept of "war", both geographically and timewise.

20. Another problem arises with armed attacks emanating from non-State actors. Although international practice has accepted that the right of self-defence extends to such attacks, the ICJ has stated that this right should not be used if the attack originates from within, and not outside, the target's own territory (since it would bring into play the territorial integrity of the other State).[31] This means that if a State recruits proxies, it will be more difficult for the target State to attribute violence to its adversary.[32]

21. The *jus in bello* (or international humanitarian law) establishes rules as to how operations may be conducted during an armed conflict. Armed conflicts are regulated not only by the Geneva Conventions of 1949 (which aim at protecting people not taking part in the hostilities) but also by international customary norms. Although the Geneva Conventions still mention the term "war", it has been widely replaced by the term "armed conflict" in international law doctrine and legal instruments (see, in particular, the 1954 Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict and its two Protocols of 1954 and 1999).

22. An armed conflict may be of international (IAC) or non-international character (NIAC). IAC is defined in common Article 2 of the Geneva Conventions and in Article 1 Section 4 of the Additional Protocol I, while NIAC is defined in common Article 3 and in Article 1 Section 1 of Additional Protocol II. Common Article 2 of the Geneva Conventions states that an IAC is a "declared war or … any other armed conflict which may arise between two or more States". Common Article 3 to the Geneva Conventions applies to "armed conflicts not of an international character occurring in the territory of one of the High Contracting Parties" (NIACs). It is generally agreed that two requirements must be met: 1) a minimum level of intensity, meaning that the hostilities must be of a "collective character" or the government must have to use military force rather than police force; and 2) the non-governmental groups must be "parties to the conflict". This means the groups must be organised, have a command structure, and conduct military operations.[33]

23. If a hybrid war qualifies as an IAC, questions of attribution under international humanitarian law and human rights law are more straightforward. As the threshold for the applicability of the law of IAC is low, a hybrid adversary is likely to deny its involvement in such an armed conflict or to avoid direct involvement in combat operations. If hostilities are unavoidable, it is in the interest of the adversary using hybrid tactics to employ proxies in order to conceal its own involvement. Then the legal regulation for NIAC, which is less

---

30. ICJ, judgment of 27 June 1986, paragraph 195: "… an armed attack must be understood as including not merely action by regular armed forces across an international border", but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to" (***interalia)*** an actual armed attack conducted by regular forces, "or its substantial involvement therein".

31. ICJ, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion of 9 July 2004, paragraph 139.

32. A. Sari, *supra* note 11, p. 25.

33. International Committee of the Red Cross (ICRC), How is the Term "Armed Conflict" Defined in International Humanitarian Law?, Opinion Paper, March 2008, p. 3. Moreover, Article 1 Section 1 of the Additional Protocol II to the Geneva Conventions defines NIACs (more narrowly) as conflicts "which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol".

demanding than that of IAC, would apply. Practice shows that States are usually reluctant to recognise the existence of a NIAC, which weakens even more the position of the target State and implies that the conflict should be treated as a domestic one.

24. Nowadays, formally declared wars are rare in international relations. However, neither a formal declaration of war nor the formal recognition of a state of war is necessary to trigger international humanitarian law (see, for instance, Articles 2 and 3 of the Geneva Convention IV). Interestingly, States no longer have the monopoly over violence; the number of inter-States conflicts has decreased, but the number of non-international armed conflicts (NIAC) has considerably increased. Many NIAC have been internationalised by the intervention of other States in support of one or more of the warring parties. Technological progress has rendered contemporary conflicts more asymmetrical.

25. In case of an armed conflict – including a "hybrid war" – both international humanitarian law and international human rights law apply. The European Court of Human Rights has clarified that, in exceptional circumstances, the Convention can be applied extraterritorially, including in cases concerning armed conflicts outside the Council of Europe's geographical area.[34] However, the application of human rights law is constrained by international humanitarian law, which operates as *lex specialis*.[35] Consistently with the case law of the ICJ, in *Hassan v. the United Kingdom,* the Court has stressed that "even in situations of international armed conflict, the safeguards under the Convention continue to apply, albeit interpreted against the background of the provisions of international humanitarian law".[36] When violations of international humanitarian law occur, States are under an obligation to prosecute alleged offenders under domestic law. In addition to this, such violations can also be prosecuted by various international criminal tribunals. However, as stressed by Mr Kozik at the November 2017 hearing, international humanitarian law has legal gaps and a weak enforcement mechanism.

2.2.2. Hybrid threats

26. In case of "hybrid threats", which do not cover military actions falling within the scope of international humanitarian law, States should deal with most of such threats through domestic criminal law (including the provisions on terrorist crimes) and human rights framework. Depending on the type of threat, a patchwork of international legal instruments covering specific policy areas (such as law of the sea, counterterrorism, hate speech, money laundering and terrorist financing) would also apply.

27. In the event of large-scale hostile non-military actions such as misinformation campaigns, it is possible to invoke Article 17 of the European Convention on Human Rights, which prohibits the abuse of rights guaranteed by the Convention. As stressed by Mr Kozik, a State Party may therefore lodge an inter-State application before the European Court of Human Rights against another State Party under Article 33 of the Convention, but Article 33 would not be applicable in cases against proxies employed by adversaries using hybrid tactics.

28. As regards cyberattacks, it is not clear how existing law is applied in cyberspace and how States should respond to cyberattacks, for which there is not even a uniformly accepted definition.[37] In 2013, the United Nations Group of Governmental Experts issued a report in which it declared that international law applies to cyberspace. Two years later, it followed up with a consensus report on norms, rules or principles of the responsible behaviour of States in the cybersphere, including a commitment to "non-intervention in the internal affairs of other States".[38] The Convention on Cybercrime of the Council of Europe of 2001 (ETS No.

---

34. See cases concerning international military operations in Iraq: *Al-Sadoon and Mufdhi v. the United Kingdom,* Application No. 61498/08, judgment of 2 March 201; *Al-Skeini and Others v. the United Kingdom,* Application No. 61498/08, and *Al-Jedda v. the United Kingdom,* Application No. 55721/07, judgment of 7 July 2011 (Grand Chamber). See also a case concerning Turkish soldiers' intervention in Iran: *Pad and Others v. Turkey*, Application No. 60167/00, judgment of 28 June 2007.

35. ICJ, *Legality of the Threat of Nuclear Weapons,* Advisory Opinion, 8 July 1996, ICJ Reports 1996, paragraph 25. See also Noam Lubell, Challenges in applying human rights law to armed conflict, *International review of the Red Cross*, Vol. 87/860, December 2005.

36. European Court of Human Rights, *Hassan v. the United Kingdom,* Application No. 29750/09, judgment of 16 September 2014, paragraphs 102-103.

37. Bruce H. McClintock, Russian Information Warfare: A Reality That Needs a Response, 21 July 2017. The ICRC, for instance, defines it as any hostile measures against an enemy designed "to discover, alter, destroy, disrupt or transfer data stored in a computer, manipulated by a computer or transmitted through a computer"; see at https://www.icrc.org/en/document/cyber-warfare.

38. United Nations, Reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013, and A/70/174, 22 July 2015.

185), is the only binding international instrument in this field. It is also open to non-member States and serves as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international co-operation.

29. In February 2017, the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations was published. This publication, drafted by a group of 19 international law experts under the auspices of NATO's Cooperative Cyber Defence Center of Excellence (based in Tallinn, Estonia), is a non-binding effort to codify the application of international law to cyberspace. However, it represents its authors' views (and not the official position of NATO) and the experts were not able to agree on how international law applies to specific situations (for example on the alleged Russian hack of the US Democratic National Committee in 2016). As stressed by Mr Kozik at the November 2017 hearing, although international humanitarian law prohibits direct attacks against civilian population and civilian objectives, its application does not preclude all types of cyberactions against them. The majority of the authors of the Tallinn Manual 2.0 were of opinion that at least functional damage (for example an electricity blackout) was needed to consider a cyberoperation as an "attack" under international humanitarian law. According to the International Committee of the Red Cross (ICRC), international humanitarian law definition of "attack" applies to cyberattacks, but this opinion remains contentious among international legal scholars[39] and it is not clear in which situations a State can invoke right of self-defence in case of a cyberattack. As a minimum, States must be allowed to take all proportionate measures necessary to avert ongoing or imminent harmful consequences of a cyberattack.

2.3. Legal gaps and possible solutions

30. By concealing its indirect involvement in the conflict, using force through proxies and conducting its operations at a level of intensity that circumvents the relevant legal thresholds, a hybrid adversary may employ armed forces against another State, while impeding the target State's ability to use force in its own defence. This creates legal asymmetry. The use of law in support of warfare is not a novelty (for instance, the Japanese invasion of Manchuria in 1931 presents many similarities to the Russian annexation of Crimea in 2014). According to Mr Sari, countering these legal challenges involves three tasks (which, so far, have not been explored by NATO and the European Union): 1) developing a definition of the legal dynamics of hybrid threats; 2) understanding legal vulnerabilities; and 3) strengthening preparedness, deterrence and defence in the legal domain.[40]

31. Concerning the first proposal, it should be stressed that legal asymmetry is a distinguishing feature of "hybrid warfare". Concerning legal vulnerabilities and challenges, it should be recalled that against actions amounting to an armed attack, the target State may use force in self-defence. The Council of Europe has clearly no competence in this field, as "national defence matters" are excluded from the scope of its activities on the basis of Article 1.*d* of its Statute (ETS No. 1). However, as many member States of our Organisation are members of NATO and/or the European Union, it will be useful to have a look at the legal means they dispose of in the event of an armed attack.

32. In the event of an armed attack against a member of NATO, Article 5 of the North Atlantic Treaty, allowing for a collective response, engages. This provision also extends to terrorist attacks directed against an allied nation from abroad.[41] Hybrid threats which do not reach the threshold of an armed attack may be addressed on the basis of Article 4 of the North Atlantic Treaty, which stipulates that NATO members may consult together whenever the territorial integrity, political independence or security of any of them is threatened. In general, States shall be able to counter hybrid threats by the use of proportionate countermeasures (reprisals).

33. In the European Union, Article 42 paragraphs 1 and 2 of the Treaty on European Union (TEU) stipulates that the "common security and defence policy shall be an integral part of the common foreign and security policy" and "shall include the progressive framing of a common Union defence policy" (the establishment of which needs a decision of the European Council). Article 42.6 of the TEU allows member States whose military capabilities fulfil higher criteria to establish permanent structured co-operation (PESCO). Such a permanent co-operation was established by a decision of the Council of the EU on 8 December 2017. Moreover, Article 42.7 of the TEU contains a mutual assistance clause in case of armed aggression, but its scope remains unclear.

39. https://www.icrc.org/en/document/cyber-warfare and https://ccdcoe.org/cycon/2012/proceedings/d3r1s1_schmitt.pdf.
40. A. Sari, *supra* note 11, pp. 26-27.
41. NATO, press release (2001)124 of 12 September 2001.

34. NATO and the European Union should work closely to find a common definition of the legal dynamics of hybrid threats and a common understanding of the legal vulnerabilities and challenges that affect them, including the legal asymmetry created by the use of hybrid tactics, challenges to the international legal order and the institutional division of labour for countering hybrid threats. Both organisations should also strengthen their legal preparedness, deterrence and defence. Both organisations have already undertaken work on countering hybrid threats.[42] For example, in April 2017, they established the European Excellence Centre for Countering Hybrid Threats, an intergovernmental think tank based in Helsinki, with 13 member States and representatives of the European Union and NATO.

3. To what extent can hybrid threats justify restrictions on human rights?

35. When countering hybrid threats (and in particular hybrid warfare), States Parties to the European Convention on Human Rights can refer to its Article 15.1, which allows States Parties to derogate from their obligations under the Convention in time of war or "other public emergency threatening the life of the nation". Such derogation should be done "to the extent strictly required by the exigencies of the situation" and should not be inconsistent with other obligations under international law. States cannot derogate from certain rights: the right to life (except in respect of deaths resulting from lawful acts of war), the prohibition of torture and inhuman or degrading treatment or punishment, the prohibition on slavery and forced labour, the principle of "no punishment without law", the prohibition of the death penalty, and the right not to be tried or punished twice. When a State derogates from the Convention, it must inform the Secretary General of the Council of Europe. Following the judgment of the European Court of Human Rights in *Hassan v. the United Kingdom,*[43] a formal derogation under Article 15 of the Convention may not be needed in cases where international humanitarian law applies, as the Convention must be interpreted in accordance with other rules of international law, including international humanitarian law. Recently, France, Ukraine and Turkey have made derogations under Article 15 of the Convention.[44]

36. States usually invoke "national security" when countering hybrid threats. Under the Convention, national security (along with, *inter alia*, "public safety" and "prevention of crime or disorder") is seen as a "legitimate aim" allowing States to limit certain rights: the right to respect for private and family life, freedom of expression and freedom of assembly and association (see paragraph 2 of Articles 8, 10 and 11 of the Convention) as well as freedom of movement (Article 2.3 of Protocol No. 4 to the Convention (ETS No. 46)); this right might also be restricted for the "maintenance of *ordre public*"). Moreover, it can justify the expulsion of an alien lawfully residing in the territory of a State without respecting the procedural safeguards (Article 1.2 of Protocol No. 7 to the Convention (ETS No. 117)). "Territorial integrity" constitutes another legitimate aim for restricting freedom of expression. Any restriction of the above rights shall be "prescribed by law", "necessary in a democratic society" and proportionate. An additional safeguard against abuses is included in Article 18 of the Convention, which stipulates that the restrictions permitted under the Convention "shall not be applied for any purpose other than those for which they have been prescribed".

37. The European Court of Human Rights has examined numerous cases in which States invoked "national security" to restrict certain human rights. The term in question is not clearly defined and remains somewhat vague, bearing in mind the margin of appreciation which States have in this sphere. The Court has assigned some substance to it by applying it to cases concerning protection of State security and constitutional democracy from espionage, terrorism, support for terrorism, separatism and incitement to breach military discipline. It now tends to require national bodies to verify that any invoked threat has a reasonable basis and carefully verifies the quality of law, the need for interference or its proportionality to the threat against "national security". Below I will refer to some relevant examples of the Court's case law concerning Articles 8, 10 and 11 of the Convention.[45]

38. Secret surveillance is among the most important cases in which "national security" has been invoked. The Court takes the view that laws on which such interference is based shall not only be "accessible" and "foreseeable", but also quite detailed. It stresses that States must show that there are adequate and effective guarantees against abuses and weighs States' interests in protecting their national security against the seriousness of the interference with the rights enshrined in Article 8 of the Convention. In *Roman Zakharov v. Russia*, concerning blanket surveillance of phone communications based on anti-terrorism law, the Court found shortcomings in the legal framework and stated that there was "the risk that a system of secret

42. For more information, see EPRS, Countering hybrid threats: EU-NATO cooperation, Briefing, May 2017.
43. *Hassan v. the United Kingdom,* op. cit., paragraphs 102-103.
44. See Assembly Doc. 14506, report on "State of emergency: proportionality issues concerning derogations under Article 15 of the European Convention on Human Rights" (rapporteur: Mr Raphaël Comte, Switzerland, ALDE).
45. European Court of Human Rights, report of the Research Division: National security and European case-law, p. 5.

surveillance set up to protect national security might undermine or even destroy democracy under the cloak of defending it" (violation of Article 8 of the Convention).[46] Interestingly, the Court is now examining a number of cases concerning the bulk interception of external communications by the United Kingdom intelligence services and the sharing of intelligence between the United Kingdom and the United States, as revealed by Edward Snowden.[47]

39. Concerning freedom of expression, there is a trend in the Court's jurisprudence not to find violations of Article 10 in cases involving the prohibition of clear and unambiguous calls to violence. The right to freedom of expression is not a right to incite violence.[48] The Court even tends, under Article 17 of the Convention, to exclude from its protection comments amounting to hate speech and negating the fundamental values of the Convention.[49] Recently, the Court has also acknowledged the importance of the internet when individuals exercise their right to freedom to receive and impart information and has examined measures blocking access to internet. In the cases *Ahmet Yildirim v. Turkey* (concerning a court decision to block access to Google Sites) and *Cengiz and Others v. Turkey* (concerning wholesale blocking of access to YouTube), it found violations of Article 10 of the Convention;[50] however, "national security" was not examined in these two cases, as the Court found that the restrictions were not "prescribed by law" and did not examine other criteria stemming from the second paragraph of Article 10.

40. In *Stankov and the United Macedonian Organisation Ilinden v. Bulgaria,* concerning the ban on assemblies organised by the applicant association aiming at "the recognition of the Macedonian minority in Bulgaria", the authorities invoked *inter alia* national security to justify the contested measure. The European Court of Human Rights declared that "demanding territorial changes in speeches and demonstration does not automatically amount to a threat to the country's territorial integrity and national security".[51] The Court found little evidence of widespread incitement to violence or undermining of democratic principles and held that safeguarding democratic institutions and practices was just as important as responding to national security concerns (violation of Article 11 of the Convention).

41. In an Issue Paper on "The rule of law on the Internet and in the wider digital world", the Council of Europe Commissioner for Human Rights concluded that "States that want to interfere with fundamental rights on the basis of an alleged threat to national security must demonstrate that the threat cannot be met by means of ordinary criminal law, including special anti-terrorist laws that still fit within the accepted parameters of criminal law and procedure and that meet international standards for criminal law and procedure". This is also valid for State actions affecting the internet and e-communications. Non-respect of the above requirement "violates the international rule of law".[52]

4. Conclusion

42. The phenomenon of "hybrid threats" requires careful attention. Although this term is widely used, its legal implications are less well understood. From the legal point of view, however, what is at stake here is the enforcement of international law norms such as prohibition of the use of force, international humanitarian law and human rights law, more than the definition of this phenomenon. There is no "law of hybrid warfare", but there are various definitions of the "hybrid war(-fare)". Most of the experts agree that the main feature of this phenomenon is legal asymmetry. Hybrid adversaries exploit lacunas in the law and legal complexity, operate across legal boundaries and under-regulated spaces, exploit legal thresholds limiting responses, and are prepared to commit substantial violations of the law under cover of legal and factual ambiguity. They deny their hybrid operations in order to create a legal grey zone within which they can operate freely. The legal regulation of "hybrid warfare" is a challenge, because one of the parties is deliberately seeking to evade its legal responsibilities.

---

46. *Roman Zakharov v. Russia*, Application No. 47143/06, judgment of 4 December 2015 (Grand Chamber), paragraph 232.
47. *Big Brother Watch and Others v. the United Kingdom,* Application No. 58170/13; *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom,* Application No. 62322/14, and *10 Human Rights Organisations and Others v. the United Kingdom,* Application No. 24960/15.
48. *Zana v. Turkey*, Application No. 18954/91, judgment of 25 November 1997, paragraph 60.
49. See, for example, *Seurot v. France,* Application No. 57383/00, admissibility decision of 18 May 2004.
50. *Ahmet Yildirim v. Turkey*, Application No. 311/10, judgment of 18 December 2012, and *Cengiz and Others v. Turkey*, Applications Nos. 48226/10 and 14017/11, judgment of 1 December 2015.
51. *Case of Stankov and the United Macedonian Organisation Ilinden v. Bulgaria*, Applications Nos. 29221/95 and 29225/95, judgment of 2 October 2001, paragraph 97.
52. Council of Europe, Commissioner for Human Rights, The rule of law on the Internet and in the wider digital world, Issue Paper, December 2014, p. 108.

43. The national security concerns of States about hybrid threats are legitimate, particularly when considering the unique ways in which hybrid threats can undermine the very core of our democratic societies. In the absence of strict internationally recognised limitations on the use of the wide range of hybrid means of waging conflict, domestic criminal law measures attempt to tackle these novel threats. Some of the domestic measures taken in response to hybrid threats may in turn violate fundamental rights. Although hybrid threats are seen as a new type of danger, the European Convention on Human Rights still applies and the Court's case law responds to questions arising around these new phenomena. Human rights concerns related to combating hybrid threats may be tackled following the approach applied to counterterrorism measures. States' responses to hybrid threats should be lawful and proportionate. In case of doubt, States can always request the expertise of the European Commission for Democracy through Law (Venice Commission) on specific pieces of draft legislation. As regards freedom of expression, some restrictions aimed at controlling the content of news may be imposed (especially to combat hate speech), but they should not be discriminatory or lead to general censorship. There are also other difficulties: it is not always possible to identify the hybrid adversary and to attribute responsibility for hybrid threats to a specific country. Moreover, phenomena such as misinformation campaigns may also imply a conflict between certain human rights and fundamental freedoms such as freedom of expression, on one hand, and the right to information and the right to free elections (as guaranteed in Article 3 of Protocol No. 1 to the Convention (ETS No. 9)), on the other hand.

44. A response to hybrid threats should include legal, counterintelligence, diplomatic and military means. Although it is not competent in defence matters, the Council of Europe should get involved in designing legal responses, contributing its human rights expertise whilst relying on the defence experience of the European Union and NATO. Not only do hybrid threats, and certain measures taken in response, pose a danger to fundamental rights, but the current legal "grey area" surrounding these new threats also undermines legal co-operation based on mutual trust and common understanding of applicable rules. The use of hybrid threats may also have legal consequences on the status of some groups of persons such as those belonging to national minorities.

45. When countering hybrid threats, States could refer to the experience they gained when fighting terrorism. International institutions and State law-enforcement agencies have engaged extensively with the threat of terrorism and there is a particular awareness of the transnational and evolving nature of non-State actors that appears throughout international treaties (such as the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196)) and domestic criminal laws relating to terrorism. The Council of Europe has developed a comprehensive framework that aims to promote and monitor fundamental rights in the fight against terrorism.[53] This framework could serve as a model for countering hybrid threats, in full respect of human rights. Moreover, the Council of Europe should promote further ratifications of the Convention on Cybercrime both by member and non-member States and engage a reflection on how it is applied and whether it needs to be improved.

53. See, for example, Assembly Resolutions 2045 (2015) "Mass surveillance" or 2090 (2016) "Combating International terrorism while protecting Council of Europe standards and values". For a more comprehensive review, refer to http://www.coe.int/en/web/counter-terrorism/codexter.