УДК 327.88 **DOI: 10.34670/AR.2019.44.5.024**

Категории гибридной войны и гибридных угроз в политологических исследованиях

Попов Павел Валентинович

Аспирант кафедры «Менеджмент организаций»,
Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова,
190005, Российская Федерация, Санкт-Петербург, ул. 1-я Красноармейская, 1;
e-mail: pa052vel@rambler.ru

Аннотация

В рамках гибридных угроз противником могут одновременно использоваться комбинации традиционных и иррегулярных методов ведения войны, наряду с политическими, военными, экономическими, социальными и информационными средствами. В статье проведен анализ понятий «гибридная война», «гибридные боевые действия» и «гибридные угрозы», их эволюция и концептуальное сходство и различие на основе нормативно-правовых документов ведущих стран мира и, в частности НАТО, регламентирующих деятельность по противодействию гибридным угрозам. Дана целевая характеристика гибридных угроз, исследованы ненасильственные стратегии современной международной политики и их использование для изменения сложившегося статуса-кво. Определены способы гибридной деятельности: военной и невоенной, традиционной и иррегулярной, явной и скрытой, государственной и негосударственной. Дан подробный обзор тематических областей гибридных угроз: политические акторы, религиозные группы, научные группы, неправительственные организации, средства массовой информации, территориальные нарушения, шпионаж, кибер-операции, угроза или применение силы, энергетическая зависимость, взяточничество и коррупция, агитация к подстрекательству, нарушение правовой системы, обострение национальных разногласий. Исследовано влияние гибридных угроз и гибридных войн на принятие политических решений и вызовы национальной безопасности.

Для цитирования в научных исследованиях

Попов П.В. Категории гибридной войны и гибридных угроз в политологических исследованиях // Теории и проблемы политических исследований. 2019. Том 8. № 5А. С. 90-98. DOI: 10.34670/AR.2019.44.5.024

Ключевые слова

Гибридные угрозы, гибридная война, гибридные боевые действия, НАТО, государственный актор.

Введение

Является системно исследованным в современных работах использование широкого спектра инструментов для достижения стратегических целей без прямой межгосударственной войны [Hoffman, 2011]. Однако характер боевых действий продолжает развиваться, предлагая противникам новые возможности для использования спектра конфликтов, выходящих за рамки применения силы, которые появляются в ходе продолжающейся информационной революции [Berkowitz, 1995].

После активного введения в категорический аппарат безопасности само определение «гибридной угрозы» и его близкие значения «гибридная война» и «гибридные военные действия» изменились вместе с конфликтами, для описания которых они использовались [Nemeth, 2002; Cullen, Reichborn-Kjennerud, 2016]. Одним из главных препятствий для четкого осмысления «гибридных» проблем является категорическое определение данной категории. Понятия «гибридные угрозы», «гибридные боевые действия», «гибридная деятельность», «гибридные операции», «гибридная тактика» и другие, часто используются взаимозаменяемо без определения [Dubik, 2018]. Более широко используются термины «боевые действия в серой зоне» [Mazarr, 2015], «конкуренция на грани войны», «современные политические боевые действия», а другие часто сливаются в академической литературе, политических публикациях и основных средствах массовой информации [Fridman, 2018]. Это находит свое отражение в разнообразии контекстов, в которых «гибридные» термины используются в политическом дискурсе и в продолжающемся обсуждении в научном сообществе. Например, Организация североатлантического договора (North Atlantic Treaty Organization, NATO, НАТО) определяет гибридные угрозы как «тип угрозы, которая сочетает в себе обычные, иррегулярные и асимметричные действия во времени и пространстве».

В статье не рассматривается вопрос внесения окончательной ясности в понятие «гибридная угроза», но затрагиваются основные проблемы безопасности, концентрируясь на характеристиках гибридных угроз. Для целей данного исследования гибридные угрозы – это действия, которые:

– скоординированы и синхронизированы;
– целенаправленно нацелены на системные уязвимости демократических государств и институтов;
– используют широкий спектр средств;
– используются на границе между возможностями обнаружения угрозы и установления инициатора воздействия, а также на границе между войной и миром;
– влияют на различные формы принятия решений на местном (региональном), государственном или институциональном уровне;
– приносят пользу и/или достигают стратегических целей при подрыве и/или нанесении ущерба цели [Treverton,Thvedt, Chen, Lee, McCue, 2018].

Основная часть

Большинство современных определений гибридных угроз в значительной степени опираются на исследования действий России в Украине и Крыму [Fridman, 2018], но при этом существует риск игнорирования одного из ключевых аспектов гибридных угроз: адаптивности.

Гибридные угрозы не следуют установленному шаблону и могут генерироваться широким кругом акторов, творчески использующих любые доступные средства и меры для достижения своих стратегических целей. Противник предпочитает избегать порога обычной войны, но может в конечном итоге прибегнуть к прямому применению силы. Следует ожидать, что будущие угрозы будут развиваться таким образом, когда противники будут приспосабливать свои средства и меры к уязвимости целевого государства.

Термин «гибридные угрозы» эволюционировал в процессе использования, распространяясь в последние годы, в частности, во всех документах Евроатлантической стратегии безопасности. Например, в регламентных документах НАТО есть «Стратегия противодействия гибридным угрозам», в ЕС разработан «Учебник» для противодействия гибридным угрозам], а Европейский центр передового опыта по противодействию гибридным угрозам был запущен в Хельсинки в 2017 г. В обзоре стратегической обороны и безопасности Великобритании за 2015 г. «гибридные угрозы» были классифицированы как «первый уровень» риска для национальной безопасности и «гибридные атаки» на союзников как «второй уровень». Все они, по существу, описывают ненасильственные стратегии в современной международной политике, направленные на выявления у противника уязвимых мест в обществе, которые будут использоваться для постепенного достижения целей, не вызывая решительных ответных мер.

Эти стратегии направлены на размывание и использование ряда различий, лежащих в основе применения силы, таких как: мир и война; международный и немеждународный конфликт; агрессия, применение силы и вооруженный конфликт. Гибридные агрессоры могут воспользоваться любой из этих «серых зон» для устранения или ограничения способности жертвы решительно реагировать, например, используя средства, которые не соответствуют определениям «силы» или «вооруженной агрессии», полагаясь на доверенных лиц для поддержания дистанции от незаконных действий или просто отрицая ответственность и ставя под сомнение фактические события, отсюда и термин «серая зона» [Dubik, 2018; Mazarr, 2015]. Эта задача ставится в контексте «межгосударственной стратегической конкуренции» и «активизации усилий, не связанных с вооруженным конфликтом». Этот тип стратегии также используется в различной степени для регионального влияния Китаем (который использует общественное мнение, психологические и правовые боевые действия в Южно-Китайском море) и Ираном (который использует широкий спектр невоенных и около-военных средств для влияния в сирийском конфликте и на Ближнем Востоке).

Широкий спектр средств и способов проявления гибридной деятельности: военной и невоенной, традиционной и иррегулярной, явной и скрытой, государственной и негосударственной, можно рассмотреть в виде тематических областей. Тематические области охватывают действующих лиц, каналы и средства. При этом они пересекаются, поскольку враждебное влияние обычно затрагивает более одной тематической области. Так, актором могут выступать политические акторы, вооруженные силы, организованные преступные группы, религиозные группы, научные группы, неправительственные организации, спонсируемые или каким-либо образом поддерживаемые государством. Канал - это система или среда, которую использует актор, например, политика, гражданское общество, военные, разведывательные, культурные, экономические или научные круги, СМИ, киберсреда, правовая система, предписывающие определенные условия, принципы и правила поведения. Средства описывают конкретные меры, применяемые актором через определенный канал: это может быть, например, дезинформация, кибератаки или нарушение закона, использование экономических рычагов, подкуп, угроза применения силы, шпионаж, агитация, территориальные нарушения.

Независимо от того, являются ли гибридные угрозы формой «войны», необходимо учитывать необходимость противодействия этому типу стратегии. В качестве потенциальных рычагов, доступных любому будущему противнику, желающему провести «гибридную» кампанию, необходимо обозначить использование следующих тематических областей угрозы:

1. Политический актор – деятельность, которая включает в себя политическую фигуру, партию или организацию, которая финансируется, организуется или направляется источником, враждебным целевой нации.
2. Территориальное нарушение международно закрепленного правового принципа территориальной целостности, который распространяется на всю территорию суши, моря и воздуха.
3. Шпионаж для получения разведанных, а также проникновение в организации или учреждения, имеющие широкие возможности по продвижению благоприятного влияния для страны-агрессора.
4. Неправительственные организации (НПО), которые официально независимы от национальных и международных правительственных организаций, но предположительно финансируются, организуются или направляются враждебным актором, или распространяют враждебную идеологию.
5. Эксплуатация этнической или культурной самобытности, обострение существующих общественных разногласий с целью воздействия на группы идентичности для того, чтобы они действовали в интересах враждебного государственного актора против интересов целевой нации.
6. Средства массовой информации целенаправленно используются с целью воздействия на аудиторию и достижения изменения отношения или поведения, которое выгодно противнику.
7. Нарушение правовой системы с помощью эксплуатация реальных, предполагаемых или даже манипулируемых случаев нарушения международного права в целях нанесения ущерба, делегитимизации политических сил или оказания влияния на общественные отношения.
8. Поощрение граждан целевой нации с помощью агитации к подстрекательству или участию в массовых демонстрациях, протестах и гражданских волнениях с целью подрыва правительства.
9. Кибер-операции, осуществляемые для захвата или искажения информационного пространства в целевом государстве.
10. Религиозные группы – актор, идентифицированный как связанный с религиозным учреждением, движением или группой, пропагандирующей враждебную религиозную доктрину или идеологию.
11. Научные группы – актор, идентифицированный как связанный с академическим учреждением или группой образовательных интересов, действующий в интересах страны-агрессора.
12. Принуждение посредством угрозы или применения силы, с целью заставить целевое государство действовать определенным образом или ограничить свободу действий.
13. Энергетическая зависимость может быть использована для экономического ослабления целевой нации или принуждения целевой нации к действиям против ее собственных национальных интересов. Это может быть сделано в ущерб национальной безопасности последнего или в нарушение международного права.

14. Взяточничество и коррупция – получение или предложение какого-либо неправомерного вознаграждения актором внутри страны-объекта с целью повлиять на его поведение, в частности побудить его действовать вопреки своим профессиональным обязательствам и вопреки интересов национальной безопасности своей страны.

Способ, которым гибридные угрозы интерпретируются и приписываются, является сложным и существенно зависит от контекста. Например, нарушение воздушного пространства может рассматриваться как случайный или преднамеренный провокационный акт. Военные учения могут восприниматься как запугивание или сдерживание, а финансируемая иностранцами политическая основа может рассматриваться как содействие межкультурному обмену или подрыв демократических ценностей. Эти интерпретации приводят к оценке угроз, которые формируют отношение как общественности, так и правительственных чиновников. Решение о том, считается ли деятельность враждебной, в конечном итоге является политическим решением, принимаемым отдельными странами, причем каждое государство видит угрозы по-разному в зависимости от собственного опыта. Основная проблема реагирования на такие ненасильственные, но потенциально опасные действия заключается в том, следует ли реагировать на них как на военные действия или как на конфронтационное поведение, или же не реагировать на них вообще.

Гибридные угрозы по самой своей природе связаны с созданием эффектов, влияющих на принятие политических решений. Эти эффекты могут быть рассеянными и развиваться в течение длительного периода времени незаметно, пока не станет слишком поздно. Эта двусмысленность означает, что правительствам может быть трудно определить, приписать или публично определить, потому что ответственный актор или общее намерение неясно или намеренно скрыто [Mumford, McDonald, 2014]. Такие действия часто описываются как происходящие в «серой зоне» между миром, кризисом и войной. Зачастую маловероятно, что правительства найдут достоверные и убедительные доказательства враждебных намерений или смогут публиковать секретные сведения в поддержку своего анализа.

В связи с этим важно также отметить критическое различие между гибридными угрозами и обычным государственным управлением, которое согласуется с международными нормами и законами и поддерживает их как в преследуемых целях, так и в используемых путях и средствах, включая действия, подпадающие под категорию «политической войны».

Принимая во внимание, что как «гибридные угрозы», так и «гибридная война» характеризуют различные вызовы национальной безопасности, следует отметить следующее:

– Гибридные угрозы сочетают в себе широкий спектр ненасильственных средств воздействия на уязвимые места в обществе, чтобы подорвать функционирование, единство или волю противника, одновременно подрывая статус-кво. Такого рода стратегия используется акторами для постепенного достижения своих целей, не вызывающих решительных ответных действий, в том числе вооруженных.
– Гибридная война – это проблема, связанная с возрастающей сложностью вооруженного конфликта, когда противники могут комбинировать виды войны и невоенные средства для нейтрализации традиционной военной силы.

С одной стороны, ненасильственные стратегии акторов, хотя и не исключают использования военного инструмента в малых дозах (или косвенно, например, принуждение посредством угрозы или применения силы), все же исключают проведение вооруженного нападения – в противном случае это была бы просто «война». С другой стороны, язык «войны» и «военных действий» обладает силой, как акт насилия, чтобы заставить противника выполнить нашу волю,

что демонстрируются обычно использованием таких понятий, как «экономическая война», «война с наркотиками», «кибервойна», «lawfare – использование закона в качестве орудия войны» и т. д.

В современных исследованиях эти два термина и понятия обычно объединяются. Следует признать, что гибридные угрозы и гибридная война могут происходить одновременно, преследуемые одним и тем же противником. Кроме того, любая будущая крупномасштабная война, скорее всего, будет включать операции гибридной войны параллельно с гибридными угрозами.

Термины «гибридная война» и «гибридные угрозы» означают разные понятия. Гибридная война описывает изменение характера войны (т.е. насильственные действия во время вооруженного конфликта), в то время как гибридные угрозы исходят от ненасильственной стратегии пересмотра статуса-кво, которая стремится к выгоде, избегая репрессий через использование «серой зоны» между миром и войной.

Заключение

Таким образом, основная политическая дилемма, возникающая в связи с гибридными угрозами, заключается в том, следует ли что-либо с этим делать. Если такая враждебная деятельность может быть терпима и поглощена, то политические последствия будут минимальны. Если это требует активного противодействия, то стратегия и возможности должны быть разработаны соответствующим образом. Этот выбор зависит от того, в какой степени гибридные угрозы могут нанести ущерб национальным интересам. С одной стороны, хоть гибридные угрозы и могут в некоторой степени создавать ущерб, но они редко ставят выбор между жизнью и смертью. С другой стороны, со временем они могут привести к кумулятивному риску и нанести ущерб основам и функциям всего общества и правительства. Это может включать в себя подрыв общественного доверия к правительству, ущерб критической инфраструктуре, искажение правил и правовых норм, затруднение экономического роста или невозможность своевременного использования государственных оборонных активов.

Гибридные угрозы также можно рассматривать как активную разведку для установления уязвимостей, которые могут быть использованы в любом долгосрочном конфликте. Этот выбор должен также учитывать потенциальную потребность в ресурсах для борьбы с гибридными угрозами. Успешное противодействие этим вызовам требует тщательного обдумывания и выверенной стратегии.

Каждый вызов имеет различные последствия для оборонной политики, стратегии и потенциала на всех уровнях ведения войны. Критически важно то, что каждый из них представляет собой пробел в способности многих стран адекватно реагировать на современные угрозы, которые, вероятно, будут продолжаться и усиливаться.

Библиография

1. Hoffman, F.G. (2011), “The hybrid character of modern conflict”, in Hybrid Warfare and Transnational Threats: Perspectives for an Era of Persistent Conflict, Council for Emerging National Security Affairs, USA.
2. Berkowitz, B.D. (1995), “Warfare in the Information Age”, Issues in Science and Technology 12, no.1 (1995), 59–66.
3. Nemeth, W.J. (2002). “In Future War and Chechnya: A Case for Hybrid Warfare”, Monterey: Naval Postgraduate School, USA.
4. Cullen, P., Reichborn-Kjennerud, E. (2016), “Countering Hybrid Warfare Baseline Assessment”, Multinational Capability Development Campaign, UK.

5. Dubik, J.M. (2018), America's Global Competitions, [Online], available at http://www.understandingwar.org/report/americas-global-competitions-gray-zone-context (Accessed 1 October 2019).
6. Mazarr, M.J. (2015), Mastering the Gray Zone. Understanding a Changing Era of Conflict. Strategic Studies Institute, U.S. Army War College, Morrisville, USA.
7. US National Defense Strategy (2018), available at http://nssarchive.us/wp-content/uploads/2018/01/2018-National-Defense-Strategy-Summary.pdf (Accessed 1 October 2019).
8. Robinson, L., Helmus, T.C., Cohen, R.S., Nader, A., Radin, A., Magnuson M., and Migacheva, K. (2018), Modern Political Warfare: Current Practices and Possible Responses, Santa Monica, Calif.: RAND Corporation, USA.
9. Fridman O. (2018), Russian 'Hybrid Warfare', Hurst & Company, London, UK.
10. NATO Standardization Office (2018), AAP-6, 62, NATO Glossary of Terms and Definitions (2018 edition), available at https://standard.di.mod.bg/pls/mstd/MSTD.blob_upload_download_routines.download_blob?p_id=281&p_table_name=d_ref_documents&p_file_name_column_name=file_name&p_mime_type_column_name=mime_type&p_blob_column_name=contents&p_app_id=600 (Accessed 1 October 2019).
11. Treverton, G.F., Thvedt, A., Chen, A.R., Lee, K., McCue, M. (2018), "Addressing Hybrid Threats", Swedish Defence University, Center for Asymmetric Threat Studies, Hybrid CoE, 2018, p10.
12. NATO (2018), "NATO's response to hybrid threats", [Online], available at https://www.nato.int/cps/en/natohq/topics_156338.htm (Accessed 1 October 2019).
13. European Commission Press Release (2017), "Security and defence: Significant progress to enhance Europe's resilience against hybrid threats – more work ahead", [Online], available at http://europa.eu/rapid/press-release_IP-17-2064_en.htm (Accessed 1 October 2019).
14. EEAS (2017), "EU and NATO inaugurate European Centre of Excellence for Countering Hybrid Threats", [Online], available at https://eeas.europa.eu/headquarters/headQuarters-homepage/33119/eu-and-nato-inaugurate-european-centre-excellence-countering-hybrid-threats_en (Accessed 1 October 2019).
15. UK HMG (2015), "National Security Strategy and Strategic Defence and Security Review 2015", available at https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015 (Accessed 1 October 2019).
16. Harjanne, A., Muilu, E., Pääkkönen, J., Smith, H. (2018), "Helsinki in the Era of Hybrid Threats – Hybrid Influencing and the City", Hybrid CoE.
17. Mumford, A., McDonald, J. (2014), "Ambiguous Warfare", report produced for the Development, Concepts and Doctrine Centre, UK.
18. Hoffman, F.G. (2018), "Examining Complex Forms of Conflict", PRISM, Vol. 7 No. 4, 2018, p.30-47.
19. Wigell, M. (2019), "Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy", International Affairs 95: 2 (2019), p. 255–275.
20. Galeotti, M. (2018), "(Mis)Understanding Russia's two 'hybrid wars'", Eurozine, [Online], available at https://www.eurozine.com/misunderstanding-russias-two-hybrid-wars/ (Accessed 1 October 2019).
21. Ministry of Defence (2014), JDP 0-01, UK Defence Doctrine, 5th Edition, 2014, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/389755/20141208-JDP_0_01_Ed_5_UK_Defence_Doctrine.pdf (Accessed 1 October 2019).

The categories of hybrid warfare and hybrid threats in political science research

Pavel V. Popov

Graduate student of Management of the Organizations department,
Baltic State Technical University "VOENMEH" named after D.F. Ustinov,
190005, 1, Pervaya Krasnoarmeiskaya st., Saint Petersburg, Russian Federation;
e-mail: pa052vel@rambler.ru

Abstract

Hybrid threats evolved out of the need to revise the established world order to compensate for the strengths and weaknesses of the status quo powers, including the self-restraint in taking decisive action and using force built into the post-world war II regime of international law. Within the framework of hybrid threats, the opponent can simultaneously use combinations of traditional and

irregular methods of warfare, along with political, military, economic, social and informational means. The article analyzes the concepts of “hybrid war”, “hybrid warfare” and “hybrid threats”, their evolution and conceptual similarities and differences based on regulatory documents of the leading countries of the world and, in particular, NATO, which control activities to counter hybrid threats. The objective characteristic of hybrid threats is given, non-violent strategies of modern international politics and their use to change the status quo are investigated. The methods of hybrid activity are determined: military and non-military, traditional and irregular, overt and covert, state and non-state. A detailed overview of the thematic areas of hybrid threats is given: political actors, religious groups, scientific groups, non-governmental organizations, the media, territorial violations, espionage, cyber operations, the threat or use of force, energy dependence, bribery and corruption, agitation to incitement, violation of the law system, aggravation of national differences. The influence of hybrid threats and hybrid wars on political decision-making and national security challenges has been investigated.

For citation

Popov P.V. (2019) Kategorii gibridnoi voiny i gibridnykh ugroz v politologicheskikh issledovaniyakh [The categories of hybrid warfare and hybrid threats in political science research]. *Teorii i problemy politicheskikh issledovanii* [Theories and Problems of Political Studies], 8 (5A), pp. 90-98. DOI: 10.34670/AR.2019.44.5.024

Keywords

Hybrid threats, hybrid war, hybrid warfare, NATO, state actor.

References

1. Hoffman, F.G. (2011), “The hybrid character of modern conflict”, in Hybrid Warfare and Transnational Threats: Perspectives for an Era of Persistent Conflict, Council for Emerging National Security Affairs, USA.
2. Berkowitz, B.D. (1995), “Warfare in the Information Age”, Issues in Science and Technology 12, no.1 (1995), 59–66.
3. Nemeth, W.J. (2002). “In Future War and Chechnya: A Case for Hybrid Warfare”, Monterey: Naval Postgraduate School, USA.
4. Cullen, P., Reichborn-Kjennerud, E. (2016), “Countering Hybrid Warfare Baseline Assessment”, Multinational Capability Development Campaign, UK.
5. Dubik, J.M. (2018), America’s Global Competitions, [Online], available at http://www.understandingwar.org/report/americas-global-competitions-gray-zone-context (Accessed 1 October 2019).
6. Mazarr, M.J. (2015), Mastering the Gray Zone. Understanding a Changing Era of Conflict. Strategic Studies Institute, U.S. Army War College, Morrisville, USA.
7. US National Defense Strategy (2018), available at http://nssarchive.us/wp-content/uploads/2018/01/2018-National-Defense-Strategy-Summary.pdf (Accessed 1 October 2019).
8. Robinson, L., Helmus, T.C., Cohen, R.S., Nader, A., Radin, A., Magnuson M., and Migacheva, K. (2018), Modern Political Warfare: Current Practices and Possible Responses, Santa Monica, Calif.: RAND Corporation, USA.
9. Fridman O. (2018), Russian ‘Hybrid Warfare’, Hurst & Company, London, UK.
10. NATO Standardization Office (2018), AAP-6, 62, NATO Glossary of Terms and Definitions (2018 edition), available at https://standard.di.mod.bg/pls/mstd/MSTD.blob_upload_download_routines.download_blob?p_id=281&p_table_name=d_ref_documents&p_file_name_column_name=file_name&p_mime_type_column_name=mime_type&p_blob_column_name=contents&p_app_id=600 (Accessed 1 October 2019).
11. Treverton, G.F., Thvedt, A., Chen, A.R., Lee, K., McCue, M. (2018), “Addressing Hybrid Threats”, Swedish Defence University, Center for Asymmetric Threat Studies, Hybrid CoE, 2018, p10.
12. NATO (2018), “NATO’s response to hybrid threats”, [Online], available at https://www.nato.int/cps/en/natohq/topics_156338.htm (Accessed 1 October 2019).
13. European Commission Press Release (2017), “Security and defence: Significant progress to enhance Europe's resilience against hybrid threats – more work ahead”, [Online], available at http://europa.eu/rapid/press-release_IP-17-2064_en.htm (Accessed 1 October 2019).

14. EEAS (2017), "EU and NATO inaugurate European Centre of Excellence for Countering Hybrid Threats", [Online], available at https://eeas.europa.eu/headquarters/headQuarters-homepage/33119/eu-and-nato-inaugurate-european-centre-excellence-countering-hybrid-threats_en (Accessed 1 October 2019).
15. UK HMG (2015), "National Security Strategy and Strategic Defence and Security Review 2015", available at https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015 (Accessed 1 October 2019).
16. Harjanne, A., Muilu, E., Pääkkönen, J., Smith, H. (2018), "Helsinki in the Era of Hybrid Threats – Hybrid Influencing and the City", Hybrid CoE.
17. Mumford, A., McDonald, J. (2014), "Ambiguous Warfare", report produced for the Development, Concepts and Doctrine Centre, UK.
18. Hoffman, F.G. (2018), "Examining Complex Forms of Conflict", PRISM, Vol. 7 No. 4, 2018, p.30-47.
19. Wigell, M. (2019), "Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy", International Affairs 95: 2 (2019), p. 255–275.
20. Galeotti, M. (2018), "(Mis)Understanding Russia's two 'hybrid wars'", Eurozine, [Online], available at https://www.eurozine.com/misunderstanding-russias-two-hybrid-wars/ (Accessed 1 October 2019).
21. Ministry of Defence (2014), JDP 0-01, UK Defence Doctrine, 5th Edition, 2014, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/389755/20141208-JDP_0_01_Ed_5_UK_Defence_Doctrine.pdf (Accessed 1 October 2019).