DSIAC Defense Systems Information Analysis Center

DSIAC TECHNICAL INQUIRY (TI) RESPONSE REPORT

Hybrid Threat Frameworks and Policies

Report Number:
DSIAC-2020-1304
Completed June 2018

DSIAC is a Department of Defense Information Analysis Center

MAIN OFFICE
4695 Millennium Drive
Belcamp, MD 21017-1505
443-360-4600

REPORT PREPARED BY:
Scott Armistead and Dominic Ju
Office: DSIAC and BluePath Labs

DSIAC is sponsored by the Defense Technical Information Center, with policy oversight provided by the Office of the Under Secretary of Defense for Research and Engineering. DSIAC is operated by the SURVICE Engineering Company.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
20-06-2018	Technical Research Report	

4. TITLE AND SUBTITLE

Hybrid Threat Frameworks and Policies

5a. CONTRACT NUMBER
FA8075-14-D-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Scott Armistead and Dominic Ju

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Defense Systems Information Analysis Center (DSIAC)
SURVICE Engineering Company
4695 Millennium Drive
Belcamp, MD 21017-1505

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center (DTIC)
8725 John J. Kingman Rd.
Ft. Belvoir, VA 22060-6218

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Hybrid threats generally arise from state and nonstate actors targeting systemic vulnerabilities within a democratic government's societal, industrial, financial, etc. structures and institutions. Hybrid threats/warfare from a policy framework perspective are difficult to define as they cross civilian and military "functions." This report describes high-level frameworks and policies that have been established to address hybrid threats along with organizations that have developed them. Two Defense Systems Information Analysis Center (DSIAC) subject matter experts performed open source searches, as well as searches of various U.S. and foreign government document repositories, to find organizations, projects, documents, and articles related to hybrid threats and frameworks and policies established to address them. A compiled list of these organizations and descriptions of their materials as

15. SUBJECT TERMS
hybrid warfare, hybrid threat, hybrid warfare policy

16. SECURITY CLASSIFICATION OF: U			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Ted Welsh, DSIAC Director
U	U	U	U	33	**19b. TELEPHONE NUMBER** *(include area code)* 443-360-4600

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

ABOUT DTIC AND DSIAC

The Defense Technical Information Center (DTIC) collects, disseminates, and analyzes scientific and technical information to rapidly and reliably deliver knowledge that propels development of the next generation of Warfighter technologies. DTIC amplifies the U.S. Department of Defense's (DoD's) multibillion dollar annual investment in science and technology by collecting information and enhancing the digital search, analysis, and collaboration tools that make information widely available to decision makers, researchers, engineers, and scientists across the Department.

DTIC sponsors the DoD Information Analysis Center's (IAC's) program, which provides critical, flexible, and cutting-edge research and analysis to produce relevant and reusable scientific and technical information for acquisition program managers, DoD laboratories, Program Executive Offices, and Combatant Commands. The IACs are staffed by, or have access to, hundreds of scientists, engineers, and information specialists who provide research and analysis to customers with diverse, complex, and challenging requirements.

The Defense Systems Information Analysis Center (DSIAC) is a DoD IAC sponsored by DTIC to provide expertise in nine technical focus areas: weapons systems; survivability and vulnerability; reliability, maintainability, quality, supportability, and interoperability; advanced materials; military sensing; autonomous systems; energetics; directed energy; and non-lethal weapons. DSIAC is operated by SURVICE Engineering Company under contract FA8075-14-D-0001.

A chief service of the DoD IACs is free technical inquiry (TI) research, limited to 4 research hours per inquiry. This TI response report summarizes the research findings of one such inquiry jointly conducted by DSIAC.

ABSTRACT

Hybrid threats generally arise from state and nonstate actors targeting systemic vulnerabilities within a democratic government's societal, industrial, financial, etc. structures and institutions. Hybrid threats/warfare from a policy framework perspective are difficult to define as they cross civilian and military "functions." This report describes high-level frameworks and policies that have been established to address hybrid threats along with organizations that have developed them. Two Defense Systems Information Analysis Center (DSIAC) subject matter experts performed open source searches, as well as searches of various U.S. and foreign government document repositories, to find organizations, projects, documents, and articles related to hybrid threats and frameworks and policies established to address them. A compiled list of these organizations and descriptions of their materials as well as a bibliography of other sources related to hybrid threats and the execution of hybrid warfare are provided in this report.

Contents

1.0 TI Request

1.1 INQUIRY

What high-level frameworks or policies have been established to address hybrid threats and what organizations have developed them?

1.2 DESCRIPTION

The inquirer's colleagues are developing a conceptual framework to help policy makers better understand the complexity of hybrid threats. To start, they are interested in conceptualizations of hybrid threats, particularly high-level frameworks or categorizations that have been developed for policy makers, and the organizations that developed them.

2.0 TI Response

Hybrid threats generally arise from state and nonstate actors targeting systemic vulnerabilities within a democratic government's societal, industrial, financial, etc. structures and institutions. The vulnerabilities can be created by many things such as historical memory, legislation, old practices, geostrategic factors, strong polarization of society, technological disadvantages, or ideological differences. A wide range of means (political, economic, military, civil, and information) can be used to attack and exploit the vulnerabilities. If improperly addressed through the application of political, economic, and military tools, these situations can escalate into hybrid warfare where the role of the military and likelihood of violence increase significantly.

Hybrid threats/warfare from a policy framework perspective are difficult to define as they cross civilian and military "functions." The legal framework for countering hybrid threats is certainly a significant issue and a challenge for liberal democracies to overcome considering hybrid threats come from illiberal (partial democracy, low-intensity democracy, empty democracy, or hybrid regime) governments and nonstate actors that don't follow international/domestic laws and norms.

2.1 U.S. AND FOREIGN GOVERNMENT INSTITUTIONS DEVOTED TO HYBRID THREATS

The Defense Systems Information Analysis Center (DSIAC) staff searched open sources for documents, articles, and other information related to hybrid threats and warfare with a focus on government organizations and materials related to development of frameworks and policy

(vs. defining threats and/or courses of action to implement the policies). It should be noted that in addition to these government entities, there are numerous academia, research, think tank, etc. institutions that support them with research, analysis, and reporting on hybrid challenges and threats and provide recommendations on policy. Some of the more prominent government institutions noted in the catalogued materials are listed in Sections 2.1.1 (U.S) and 2.1.2 (European Union [E.U.] and United Kingdom [U.K.-+]).

2.1.1 U.S. Government Institutions

1. **U.S. Army Asymmetric Warfare Group (AWG).** The AWG provides operational advisory support globally and rapid solution development to the Army and Joint Force commanders to enhance Soldier survivability and combat effectiveness, and to enable the defeat of current and emerging threats in support of Unified Land Operations. http://www.awg.army.mil/

2. **U.S. Department of Homeland Security (DHS), National Consortium for the Study of Terrorism and Responses to Terrorism (START).** START is a DHS Center of Excellence headquartered at the University of Maryland. It is a university-based research and education center comprising an international network of scholars committed to the scientific study of the causes and human consequences of terrorism in the United States and around the world. It investigates fundamental questions about terrorism, including the following:

    a. What is the nature of terrorism in the world today? How has terrorist activity evolved over time? How does terrorism vary across geographies? And what do these trends indicate about likely future terrorism?

    b. Under what conditions does an individual or a group turn to terrorism to pursue its goals? What is the nature of the radicalization process?

    c. How does terrorism end? What are the processes of deradicalization and disengagement from terrorism for groups and individuals?

    d. What actions can governments take to counter the threat of terrorism?

    e. What impact does terrorism and the threat of terrorism have on communities, and how can societies enhance their resilience to minimize the potential impacts of future attacks?

    A few of START's hybrid threat-related projects are listed as follows:

    a. A Multi-Level Approach to the Study of Violent Extremism http://www.start.umd.edu/research-projects/multi-level-approach-study-violent-extremism

b. Anatomizing Radiological and Nuclear Non-State Adversaries
http://www.start.umd.edu/research-projects/anatomizing-behavior-chemical-and-biological-non-state-adversaries

c. Building a Unified Infrastructure for Data Integration on Political Violence and Conflict
http://www.start.umd.edu/research-projects/building-unified-infrastructure-data-integration-political-violence-and-conflict

d. Consensus Framework for Informing Decision-Making in the Biological Threat Characterization Program
http://www.start.umd.edu/research-projects/consensus-framework-informing-decision-making-biological-threat-characterization

e. Developing Integrated Radiological and Nuclear Detection Architecture for the Interior and International Mission Space
http://www.start.umd.edu/research-projects/developing-integrated-radiological-and-nuclear-detection-architecture-interior-and

f. Resources and Resilience: A Computational Model of Strategic Influence
http://www.start.umd.edu/research-projects/resources-and-resilience-computational-model-strategic-influence

g. Shadows of Violence: Empirical Assessments of Threats, Coercion and Gray Zones
http://www.start.umd.edu/research-projects/shadows-violence-empirical-assessments-threats-coercion-and-gray-zones

Additional information on START is available at the following links:

- START
http://www.start.umd.edu/
- START Policy & Practice
http://www.start.umd.edu/policy-practice
- START online publications reference (many related to the hybrid threat)
http://www.start.umd.edu/publications
- START relevant publications geared towards the Homeland Security enterprise
http://www.start.umd.edu/publications?type[]=10&type[]=2087&type[]=13&type[]=110&type[]=2110&type[]=9&type[]=11&type[]=15&type[]=111&type%5B%5D=111

3. **U.S. Cyberspace Solarium Commission.** This commission is tasked by the U.S. Congress with developing a consensus on a strategic approach to protecting the crucial

advantages of the United States in cyberspace. Membership includes Principal Deputy Director of National Intelligence, Deputy Director of Homeland Security, Deputy Secretary of Defense, three members appointed by Senate majority leader, two members appointed by Senate minority leader, three members appointed by Speaker of the House of Representatives, and two members appointed by minority leader of the House.
https://www.sasse.senate.gov/public/index.cfm/press-releases?ID=A75F324A-F7DC-41DE-A0FC-80A472933A28

4. **U.S. Joint Chiefs of Staff (JCS)**. The JCS consists of the Chairman, the Vice Chairman, the Chief of Staff of the Army, the Chief of Naval Operations, the Chief of Staff of the Air Force, the Commandant of the Marine Corps, and the Chief of the National Guard Bureau. These senior uniformed leaders are tasked with advising the President, the Secretary of Defense, the Homeland Security Council, and the National Security Council on military matters including hybrid threats and warfare.
http://www.jcs.mil/

5. **U.S. National Security Council (NSC)**. Since its inception under President Truman, the NSC has been the President's principal forum for considering national security and foreign policy matters with his senior national security advisors and cabinet officials. The Council also serves as the President's principal arm for coordinating these policies among various government agencies.
https://www.whitehouse.gov/nsc/

6. **U.S. Office of the Director of National Intelligence (DNI), National Counterterrorism Center (NCTC)**. The NCTC leads and integrates the national counterterrorism (CT) effort by fusing foreign and domestic CT information, providing terrorism analysis, sharing information with partners across the CT enterprise, and driving whole-of-government action to secure our national CT objectives. The NCTC operates as a partnership of organizations to include the Central Intelligence Agency; Department of Justice/Federal Bureau of Investigation; Departments of State, Defense, and Homeland Security; and other entities that provide unique expertise such as the Departments of Energy, Treasury, Agriculture, Transportation, and Health and Human Services; and the Nuclear Regulatory Commission. They develop, integrate, implement, and measure the effectiveness and progress of strategic operational plans for U.S. CT activity as well as assign roles and responsibilities to lead departments or agencies for CT activities according to strategic operational plans and consistent with applicable laws. The NCTC CURRENT serves as a secure website dissemination mechanism for terrorism information produced by NCTC and other CT mission partners. The NCTC Terrorist Identities Datamart Environment (TIDE) is the U.S. Government's central repository of information on international terrorist identities.

https://www.dni.gov/index.php/nctc-home/
NCTC Overview; 20170818; Congressional Research Service
https://fas.org/sgp/crs/intel/IF10709.pdf

7. **U.S. Senate Committee on Foreign Relations (SFRC).** The SFRC is charged with leading foreign-policy legislation and debate in the Senate. It is generally responsible for overseeing (but not administering) and funding foreign aid programs as well as funding arms sales and training for national allies.
https://www.foreign.senate.gov/

8. **Secretary of Defense (SecDef) and Office of the Secretary of Defense (OSD).** United States Code (USC) Title 10 provides that the SecDef has "authority, direction and control over the Department of Defense," and is further designated as "the principal assistant to the President in all matters relating to the Department of Defense." The same statute also ensures civilian control of the military. The SecDef is responsible for exercising command and control, for both operational and administrative purposes subject only to the orders of the President, over all Department of Defense forces. OSD is the principal staff element of the SecDef in the exercise of policy development, planning, resource management, and fiscal and program evaluation responsibilities.
https://www.defense.gov/About/Office-of-the-Secretary-of-Defense/

2.1.2 E.U. and U.K. Government Institutions

1. **The Council of the European Union.** This E.U. council represents the member states' governments; it is also known informally as the E.U. Council. National ministers from each E.U. country meet as part of this council to adopt laws and coordinate policies.
https://www.consilium.europa.eu/en/council-eu/

2. **European Council.** This E.U. institution defines the general political direction and priorities of the E.U. It consists of the heads of state or government of the member states**,** together with its President and the President of the Commission. It is also the leading human rights organization for the E.U..
https://www.consilium.europa.eu/en/european-council/

3. **European Commission (EC).** The EC is the executive of the E.U., which promotes its general interest.
https://ec.europa.eu/commission/index_en

4. **European Center of Excellence for Countering Hybrid Threats (Hybrid CoE).** This CoE serves as a hub of expertise supporting the participating countries' individual and collective efforts to enhance their civil-military capabilities, resilience, and preparedness to counter hybrid threats with a special focus on European security. It is intended that the Center will offer collective experience and expertise for the benefit of all participating countries, as well as the E.U. and NATO. It will follow a comprehensive,

multinational, multidisciplinary, and academic-based approach.
http://www.coedat.nato.int/

5. **European Defense Agency (EDA).** The EDA is an intergovernmental agency that falls under the authority of the Council of the E.U., to which it reports and from which it receives guidelines. The EDA acts as a catalyst, promotes collaborations, launches new initiatives, and introduces solutions to improve E.U. defense capabilities.
https://www.eda.europa.eu/
6. **North Atlantic Treaty Organization (NATO) Centre of Excellence for Defence Against Terrorism (COE DAT).** The COE DAT is composed of 62 multinational billets with representatives from eight nations focused on providing key decision-makers with realistic solutions to terrorism and CT challenges. It is designed to complement NATO's current resources while also serving as NATO's Department Head in Education and Training for CT.
http://www.coedat.nato.int/
7. **NATO Energy Security Center of Excellence (ENSEC COE).** This organization is composed of military and civilian experts from NATO and Partner Nations. The Steering Committee guides the activities of the Center through yearly Programmes of Work coordinated with NATO Allied Command Transformation (ACT). It assists Strategic Commands, other NATO bodies, nations, partners, and other civil and military bodies by supporting NATO's capability development process, mission effectiveness, and interoperability in the near, mid, and long terms by providing comprehensive and timely subject matter expertise on all aspects of energy security.
https://www.enseccoe.org/en
8. **UK Ministry of Defense (UK MOD) Development, Concepts and Doctrine Centre (DCDC).** This UK MOD think tank helps inform defense strategy, capability development, and operations and provides the foundation for joint education.
https://www.gov.uk/government/groups/development-concepts-and-doctrine-centre

Notable in this search was the apparent absence of a single U.S. institution tasked with addressing hybrid challenges and threats in a national, coordinated manner. The E.U. appears to be more advanced in this area with overarching governmental policies in place that have implemented such institutions. One of the most notable and active appears to be the E.U.'s Hybrid Center of Excellence (Hybrid CoE) managed by the Swedish Defense University. In April 2016, the E.U. published the "Joint Framework on Countering Hybrid Threats – a European Union Response." Initiatives within this document were the genesis of the E.U. Hybrid CoE. Later, in December 2016, a common set of proposals for implementation of the Joint Declaration by the President of the European Council, President of the European Commission, and the Secretary General of NATO for countering hybrid threats was endorsed by the Council of the European Union and the North Atlantic Council [1].

The Hybrid CoE is made up of organizations from different E.U. member countries specializing in various hybrid defense areas that are dedicated to furthering a common understanding of hybrid threats and promoting the development of comprehensive, whole-of-government response at national levels and of coordinated response at E.U. and NATO levels in countering hybrid threats. Similar to the U.S. DoD Reliance 21 initiative, the E.U. Hybrid CoE establishes a joint framework that provides solutions and advice to senior-level political leaders, policy and decision makers, and warfighters. This framework is achieved through an ecosystem and infrastructure that provides for education, information sharing, alignment of effort, coordination of priorities, and support across the E.U. government and military enterprise. Also similar to Reliance 21, the Hybrid CoE is supported by Communities of Interest (COIs). In the case of the Hybrid CoE, the COIs are managed by various member countries and include Coordination & Support, Hybrid Influencing COI (UK), Sub-COI on Non-State Actors (SWE), Strategy & Defense COI (DE), and Vulnerabilities & Resilience COI (FIN) [1−3].

2.2 HYBRID THREAT FRAMEWORKS AND OVERARCHING ACTIVITIES

Catalogued materials/references relating to hybrid threat frameworks are presented in Sections 2.2.1 (U.S) and 2.2.2 (E.U. and U.K.). For relevancy and expediency, the search was generally limited to materials dated within the past 4 years (2015 and newer). Most of the documents cited are available on request from DSIAC, if you are unable to access them through the listed links.

Note: For clarity, the documents produced by these activities/organizations are listed here under the organizations that developed them.

2.2.1 U.S. Frameworks

1. **U.S. Cyberspace Solarium Commission.**
    a. Cyberspace Solarium Commission Overview; 2018; U.S. Senator Ben Sasse, Nebraska https://www.sasse.senate.gov/public/_cache/files/cf57ede8-1b02-47c3-b41b-d3898edeb9ef/solarium-fact-sheet.pdf
    b. A Cyber Solarium Project; 20180117; LAWFARE; Klon Kitchen, Founder Kraken Wurx Strategies (technology and national security consulting company) and Fellow for National Security, Technology, Cyber, and Science, Heritage Foundation https://www.lawfareblog.com/cyber-solarium-project

2. **U.S. Joint Chiefs of Staff (JCS).** The JCS publishes overarching documents providing guidance for planning and response execution for all aspects of warfare including those related to illiberal and nonstate actor hybrid threats.

    a. Joint Concept for Integrated Campaigning (JCIC); 20180316. The JCIC establishes a framework and policies to remedy the deficiencies of U.S. legacy defense establishment processes that presuppose clearly defined states of peace and war. The goal is to improve the ability of the Joint Force to face challenges in an operating environment where hostile forces are seeking to undermine U.S. interests without triggering an overt conflict. The JCIC attempts to define integrated campaigning with participation by the U.S. Joint Force and interorganizational partners to achieve and maintain policy aims. The JCIC describes integrating military activities and aligning nonmilitary activities of sufficient scope, scale, simultaneity, and duration across multiple domains. In addition, it presents a methodology with associated capabilities that enables the Joint Force to collaborate and synchronize with interorganizational partners and conduct globally integrated operations to achieve acceptable and sustainable outcomes.
    http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257

    b. Joint Publication 3-0, Doctrine for Joint Operations; 20010910. This publication provides guidance for conducting joint and multinational activities across the range of military operations. It presents joint warfighting doctrine and establishes the framework for our forces' ability to fight as a joint team. Often called the "linchpin" of the joint doctrine publication hierarchy, Joint Publication 3-0 overarching concepts and principles provide a common perspective from which to plan and execute joint, interagency, and multinational operations. This comprehensive document addresses all key aspects of joint warfighting and military operations other than war, where many of today's military activities are focused.
    https://www.dsiac.org/resources/reference-documents/joint-publication-3-0-doctrine-joint-operations-10-sep-2001

    c. Joint Publication 3-07, Joint Doctrine for Military Operations Other Than War; 19950616. This publication describes the basic tenets of military operations other than war (MOOTW) including a general description of all types of operations and planning considerations necessary for effective execution. It is the first in a series of publications on tactics, techniques, and procedures that provide additional detail on the more complex MOOTW. Joint Publication 3-07 explains how MOOTW differ from large-scale, sustained combat operations, and it addresses purpose, principles, types of operations, and planning

considerations. A doctrinal basis is provided for related joint tactics, techniques, and procedures (JTTP) publications, which address specific types of MOOTW. https://www.dsiac.org/resources/reference-documents/joint-publication-3-07-joint-doctrine-military-operations-other-war-16

3. The U.S. White House and U.S. Secretary of Defense

    a. National Security Strategy (NSS); 201802. The NSS maintains that, in addition to the threats posed to the U.S. by rogue regimes and violent extremist organizations that have been a central focus of national security policy since the end of the Cold War, great power rivalries and competition have once again become a central feature of the international security landscape. To advance U.S. interests effectively within this strategic context, the Administration argues, the U.S. must improve domestic American security and bolster economic competitiveness while rebuilding its military. The NSS is organized into four interconnected "pillars": 1) protect the American people, the homeland, and the American way of life; 2) promote American posterity; 3) preserve peace through strength; and 4) enhance American influence. More information on the NSS is available at the following links:

        i. National Security Strategy of the United States of America; 201712; The White House https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

        ii. CRS IN10842, The 2017 National Security Strategy: Issues for Congress; 20171219; Congressional Research Service (CRS) (two-page summary of the NSS pillars and key points) https://fas.org/sgp/crs/natsec/IN10842.pdf

    b. National Defense Strategy (NDS); 20180119. The NDS articulates how the DoD will advance U.S. objectives articulated in the NSS. In addition to stating the DoD's approach to contending with current and emerging national security challenges, the NDS is also intended to articulate the overall strategic rationale for programs and priorities contained within the FY2019−FY2023 budget requests. Overall, the document maintains that the strategic environment in which the United States must operate is characterized by the erosion of the rules-based international order, which has produced a degree of strategic complexity and volatility not seen "in recent memory" (p. 1). As a result, the document argues, the United States must bolster its competitive military advantage—which the NDS sees as having eroded in recent decades—relative to the threats posed by China and Russia. It further maintains that "inter-state strategic competition, not terrorism, is now the primary concern in U.S. national

security." The NDS is a classified document; however, a summary by The White House and insights from reviews by the CRS or Library of Congress can be found at the following links:

i. Summary of the 2018 National Defense Strategy of The United States of America; 2018; U.S. Secretary of Defense https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

ii. The 2018 National Defense Strategy; 20180205; CRS (two-page summary of key points and potential questions for Congress) https://fas.org/sgp/crs/natsec/IN10855.pdf

2.2.2 E.U. and U.K. Frameworks

1. European Center of Excellence for Countering Hybrid Threats (Hybrid CoE). The establishment of the Hybrid CoE was defined in/supported by the EDA Capability Development Plan (see Framework 2 in this section) and a common set of proposals written in a joint declaration by the European Council, European Commission, and NATO in 2016. Other Hybrid CoE publications and their links are listed as follows:

   a. Common Set of Proposals for the Implementation of the Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization; 2016 https://www.hybridcoe.fi/wp-content/uploads/2017/08/Common-set-of-proposals-for-the-implementation-of-the-Joint-Declaration-2.pdf

   b. The Resurrection of 'Active Measures': Intelligence Services as a Part of Russia's Influencing Toolbox; 201804 https://www.hybridcoe.fi/wp-content/uploads/2018/05/Strategic-Analysis-2018-4-Juurvee.pdf

   c. From Nudge to Novichok: The Response to the Skripal Nerve Agent Attack Holds Lessons for Countering Hybrid Threats; 201804 https://www.hybridcoe.fi/wp-content/uploads/2018/04/HybridCoE_WorkingPaper_From-NudgeToNovichok_Omand.pdf

   d. Countering Hybrid Threats: Role of Private Sector Increasingly Important. Shared Responsibility Needed; 201803 https://www.hybridcoe.fi/wp-content/uploads/2018/03/Strategic-Analysis-2018-3-Limnell.pdf

e. Hybrid Threats as a New 'Wicked Problem' for Early Warning; 201803 https://www.hybridcoe.fi/wp-content/uploads/2018/06/Strategic-Analysis-2018-5-Cullen.pdf

f. Beyond Fake News: Content Confusion and Understanding the Dynamics of the Contemporary Media Environment; 201802 https://www.hybridcoe.fi/wp-content/uploads/2018/02/Strategic-Analysis-2018-2-February-Valaskivi.pdf

g. Blurred Lines: Hybrid Threats and the Politics of International Law; 201801 https://www.hybridcoe.fi/wp-content/uploads/2018/01/Strategic-Analysis-2018-1-January-Sari.pdf

h. Addressing Hybrid Threats; 2018 https://www.hybridcoe.fi/wp-content/uploads/2018/05/Treverton-AddressingHybridThreats.pdf

i. Laws in the Era of Hybrid Threats; 201712, 201710 https://www.hybridcoe.fi/wp-content/uploads/2018/01/HybridCoE_SA_2017_Dec_Ferm.pdf

j. Is Russia's Energy Weapon Still Potent in the Era of Integrated Energy Markets?; 201711 https://www.hybridcoe.fi/wp-content/uploads/2017/12/Strategic-Analysis-November-2017.pdf

k. In the Era of Hybrid Threats: Power of the Powerful or Power of the "Weak"?; 201710 https://www.hybridcoe.fi/wp-content/uploads/2017/12/Strategic-Analysis-October-2017.pdf

l. Regional Cooperation to Support National Hybrid Defence Efforts; 201710 https://www.hybridcoe.fi/wp-content/uploads/2017/12/hybridcoe_wp1_regional_cooperation.pdf

2. European Defense Agency (EDA), Capability Development Plan (CDP) (part of which defines E.U. priority actions for Hybrid Threats)

a. Hybrid Warfare; 201605; EDA Hybrid Warfare goals and objectives https://www.eda.europa.eu/what-we-do/activities/activities-search/hybrid-warfare

b. CDP Project Goals and Description; 20170616 https://www.eda.europa.eu/what-we-do/activities/activities-search/capability-development-plan

c. CDP Framework Description
https://www.eda.europa.eu/what-we-do/our-current-priorities/capability-development-plan

d. CDP Fact Sheet; 20170620
https://www.eda.europa.eu/docs/default-source/eda-factsheets/2017-06-20-factsheet-cdp.pdf

e. CDP Emerging Trends and Key Priorities Brochure
https://www.eda.europa.eu/docs/default-source/eda-publications/futurecapabilities_cdp_brochure

3. European Commission (EC), Joint Framework on Countering Hybrid Threats; 20160406; Parlementaire Monitor
https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vk30hn8tljz9?ctx=vga3buzdwirl&tab=1&start_tab0=240

4. Singapore Air Force (RSAF), Framework for Identifying Requirements in the Design of Multi-Domain Command & Control Information System for Tri-Service Integration; 2017; Pointer Journal
https://www.mindef.gov.sg/oms/safti/pointer/documents/pdf/V43N2a5.pdf

5. UK Ministry of Defense (UK MOD), Development, Concepts and Doctrine Centre (DCDC); The DCDC link provides information on the Multinational Capability Development Campaign (MCDC), which was designed to develop and deliver new capabilities to enhance partnerships and effectiveness in joint, multinational, and coalition operations including those in response to hybrid threats. Also, links can be found to access Allied Joint Publications (AJPs), doctrine for NATO operations; Joint Doctrine Publications (JDPs), fully endorsed national doctrine, and Joint Doctrine Notes (JDNs), which are provided to encourage debate and capture and disseminate best practices.
https://www.gov.uk/government/groups/development-concepts-and-doctrine-centre.
MCDC-related links are listed as follows:

a. Multinational Capability Development Campaign (MCDC); 20170928; UK Ministry of Defense; Multinational Capability Development College
https://www.gov.uk/government/collections/multinational-capability-development-campaign-mcdc

b. MCDC Countering Hybrid Warfare (CHW) Project - Multinational project to help understand the nature and character of modern hybrid threats.
https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare

i. MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare, 201701

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

c. MCDC Understand to Prevent (U2P) Project - Military Contribution to the Prevention of Violent Conflict; 20170620; Multinational project to determine how defence forces can prevent violent conflict https://www.gov.uk/government/publications/understand-to-prevent-the-military-contribution-to-the-prevention-of-violent-conflict

   i. MCDC Understand to Prevent (U2P) Project: the Military Contribution to the Prevention of Violent Conflict; 201411 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/518617/20150430-U2P_Main_Web_B5.pdf

   ii. MCDC Understand to Prevent (U2P) Project: the Military Contribution to the Prevention of Violent Conflict Short Guide; 201411 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/518378/20150223-MCDC_U2P_Summary_Secured.pdf

   iii. MCDC Understand to Prevent (U2P) Project: the Military Contribution to the Prevention of Violent Conflict Handbook; 201404 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/618886/dar_mcdc_u2p_handbook.pdf

2.2.3 Other Framework Documents

1. Warfare as Violent Politics: An Integrated Framework for Analyzing Armed Threats, 20180502, War on the Rocks, Director of the Combating Terrorism Fellowship Program and an Associate Professor at the College of International Security Affairs of the National Defense University https://warontherocks.com/2018/05/warfare-as-violent-politics-an-integrated-framework-for-analyzing-armed-threats/

2. Thesis: Identifying 'Hybrid Warfare'; 2016; Leiden University, Netherlands; Manon van Tienhoven (The thesis attempts to demonstrate that when using a framework of hybrid warfare perspectives to identify hybrid warfare in practice, the definitions of hybrid warfare and its elements are too general, which leads to doubt of its added value in the debate.) https://openaccess.leidenuniv.nl/bitstream/handle/1887/53645/2016_Tienhoven_van_CSM.pdf?sequence=1

2.3 HYBRID WARFARE POLICY-RELATED DOCUMENTS

Catalogued materials/references relating to hybrid warfare policy are presented in the following list. For relevancy and expediency, the search was generally limited to materials dated within the past 4 years (2015 and newer). If you are unable to access the documents through the listed links, most are available on request from DSIAC.

Additionally, other materials related to hybrid threats and warfare that may be more focused on defining the threat and operational implementation of responses are listed in Appendix A. The following references may also provide significant information on frameworks, policy, and its implementation.

1. National Security Strategy of the United States of America; 201712; The White House https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf
2. Hybrid War and Its Countermeasures: A Critique of the Literature, 20170930, University of Oxford https://www.tandfonline.com/doi/abs/10.1080/09592318.2018.1404770?src=recsys&journalCode=fswi20
3. Understanding Russian "Hybrid Warfare" and What Can Be Done About It, 20170322, RAND Corp https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf
4. HASC-115-22, The Evolution of Hybrid Warfare and Key Challenges; 20170322; Hearing Statements by Members of Congress to the House of Representatives Committee on Armed Services https://www.gpo.gov/fdsys/pkg/CHRG-115hhrg25088/pdf/CHRG-115hhrg25088.pdf
5. Review of Domestic Sharing of Counterterrorism Information; 201703; Department of Justice – presents findings and recommendations on integration, coordination, and national strategy. https://oig.justice.gov/reports/2017/a1721.pdf
6. The United States, The Russian Federation and the Challenges Ahead; 20170209; Atlantic Council and Georgia Institute of Technology, Gen (Ret) Philip M. Breedlove https://www.foreign.senate.gov/imo/media/doc/020917_Breedlove_Testimony_REVISED.pdf
7. NATO ENSEC COE #11, Hybrid Threats: Overcoming Ambiguity, Building Resilience; 2017; NATO Energy Security Center of Excellence (ENSEC COE) – This magazine contains eight articles on hybrid warfare/threats: 1) *Hybrid Threats: Overcoming Ambiguity, Building*

Resilience Expert Level Workshop; 2) What to Do with Hostile Information Campaign/Propaganda?; 3) A NATO Land Domain Perspective; 4) Hybrid Threats on Energy Infrastructures and Supply Lines; 5) The Energy Weapon That Could Not - Assessing European Energy Security in the Stand-Off with Russia, 2014-2015; 6) Energy in New Generation Warfare. Learned Lessons from Russia's Hybrid War Against Ukraine; 7) Critical Infrastructure Protection: The Challenges Connected To Working Out the Green Paper on CIP In Ukraine; and *8) Social Resilience in Lithuania: The Lithuanian Riflemen's Union Experience*.
https://enseccoe.org/data/public/uploads/2017/03/zurnalas_no11_sp_176x250mm_3mm_2.pdf

8. Countering Gray-Zone Hybrid Threats: An Analysis of Russia's 'New Generation Warfare' and Implications for the US Army; 20161018; West Point Modern War Institute, John Chambers
https://mwi.usma.edu/wp-content/uploads/2016/10/Countering-Gray-Zone-Hybrid-Threats.pdf
9. The Role of Counter Terrorism in Hybrid Warfare; 201608; NATO Centre of Excellence for Defence Against Terrorism (COE DAT) and University of Nottingham
http://www.coedat.nato.int/publication/researches/05-TheRoleofCounterTerrorisminHybridWarfare.pdf
10. Russia and Hybrid Warfare – Going Beyond the Label; 201601; Aleksanteri Papers, Bettina Renz and Hanna Smith
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=17&cad=rja&uact=8&ved=0ahUKEwjevburwc7bAhVM7YMKHWFhBUw4ChAWCE0wBg&url=https%3A%2F%2Fwww.stratcomcoe.org%2Fdownload%2Ffile%2Ffid%2F4920&usg=AOvVaw2HUcl2dQ3JTA8CEjs1yQaT
11. Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO; 201502; The German Marshall Fund of the United States, Merle Maigre
http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=23&cad=rja&uact=8&ved=0ahUKEwj2hLbmws7bAhXI6YMKHUrXC8Y4FBAWCDUwAg&url=http%3A%2F%2Fwww.gmfus.org%2Ffile%2F4272%2Fdownload&usg=AOvVaw2Qoa9xfXkJzblrQF1yMZxL
12. The National Military Strategy of the United States of America; 2015; Joint Chiefs of Staff
http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf
13. NATO's Response to Hybrid Threats, 2015; NATO Defense College (NDC)
https://www.files.ethz.ch/isn/195405/fp_24.pdf

2.4 HYBRID WARFARE POLICY-RELATED WEB ARTICLES

1. Threat Report 2018: Russia's Military Doctrine of Deception and Deniability, 20180531, The Cipher Brief https://www.thecipherbrief.com/threat-report-2018-russias-military-doctrine-of-deception-and-deniability
2. The Council of Europe's Parliamentary Assembly Takes on the Legal Challenges of Hybrid Warfare; 20180523; LAWFARE, Aurel Sari, senior lecturer in law, University of Exeter UK and Director, Exeter Centre for International Law https://lawfareblog.com/council-europes-parliamentary-assembly-takes-legal-challenges-hybrid-warfare
3. A New Blueprint for Competing Below the Threshold: The Joint Concept for Integrated Campaigning; 20150523; War On The Rocks; Phillip Lohaus, Research Fellow, American Enterprise Institute (focuses on special operations forces, the intelligence community, and competitive strategies) and previously served as an intelligence analyst in the Department of Defense. https://warontherocks.com/2018/05/a-new-blueprint-for-competing-below-the-threshold-the-joint-concept-for-integrated-campaigning/
4. PACE Warns of the New Threat of 'Hybrid War', but Reaffirms That Existing Laws Continue to Apply; 20180427; Council of Europe Parliamentary Assembly http://assembly.coe.int/nw/xml/News/News-View-EN.asp?newsid=7059&cat=8
5. Restoring Equilibrium: U.S. Policy Options for Countering and Engaging Russia; 201802; Brookings Institute, Foreign Policy, Sergey Aleksashenko and Pavel Baev https://www.brookings.edu/wp-content/uploads/2018/02/fp_201802_russia_restoring_equilibrium.pdf
6. Legal Challenges Related to the Hybrid War and Human Rights Obligations; 20180314; Council of Europe, Committee on Legal Affairs and Human Rights http://website-pace.net/documents/19838/4246196/20180314-HybridWar-EN.pdf/3387f663-0e5d-407e-a90b-9e5880474589
7. Adapting NATO to an Unpredictable and Fast-Changing World; 20180219; NATO OTAN, NATO Review Magazine; Julian Lindley-French, Senior Fellow, Institute of Statecraft in London and Distinguished Visiting Research Fellow, National Defense University in Washington and Fellow, Canadian Global Affairs Institute https://www.nato.int/docu/review/2018/Also-in-2018/adapting-nato-to-an-unpredictable-and-fast-changing-world-defence-alliance-security/EN/index.htm
8. Hybrid Operations and the Importance of Resilience: Lessons From Recent Finnish History; 20180208; Carnegie Endowment for International Peace

https://carnegieendowment.org/2018/02/08/hybrid-operations-and-importance-of-resilience-lessons-from-recent-finnish-history-pub-75490

9. New Defense Strategy Requires Paradigm Shift in US Counterterrorism; 20180127; The Hill, William Braniff and Alex Gallo http://thehill.com/opinion/national-security/370748-new-defense-strategy-requires-paradigm-shift-in-us-counterterrorism
10. Hybrid Threats and the United States National Security Strategy: Prevailing in an "Arena of Continuous Competition"; 20180119; European Journal of International Law (EJIL); Aurel Sari, Senior Lecturer in Law, University of Exeter and Director, Exeter Centre for International Law and Fellow, Allied Rapid Reaction Corps; Arnis Lauva, Third Secretary, Legal Department of the Ministry of Foreign Affairs, Latvia https://www.ejiltalk.org/hybrid-threats-and-the-united-states-national-security-strategy-prevailing-in-an-arena-of-continuous-competition/
11. Rethinking the Danger of Escalation: The Russia-NATO Military Balance; 201801; Carnegie Endowment for International Peace; Aleksandr Khramchikhin, Deputy Director, Institute for Political and Military Analysis in Moscow https://carnegieendowment.org/files/Khramchikhin_NATO_web.pdf
12. 2018 Defence White Paper: Investing in Our People, Capabilities and Visibility; 2018; Netherlands Ministry of Defence https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=69&ved=0ahUKEwiFvv2b4cHbAhVDLKwKHflMBQc4PBAWCFowCA&url=https%3A%2F%2Fenglish.defensie.nl%2Fbinaries%2Fdefence%2Fdocuments%2Fpolicy-notes%2F2018%2F03%2F26%2Fdefence-white-paper%2FDefence%2BWhite%2BPaper%2B2018.pdf&usg=AOvVaw1pPtgzFVKj3DpyLtC2QiT3
13. U.S. Presence and the Incidence of Conflict; 2018; RAND Corp https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1906/RAND_RR1906.pdf
14. Hybrid Warfare: Aggression and Coercion in the Gray Zone; 20171129, American Society of International Law, LT Douglas Cantwell, USN, Judge Advocate General's Corps https://www.asil.org/insights/volume/21/issue/14/hybrid-warfare-aggression-and-coercion-gray-zone
15. Russia's Neighbors Respond to Putin's 'Hybrid War'; 20171012; Foreign Policy, Reid Standish, Associate Editor http://foreignpolicy.com/2017/10/12/russias-neighbors-respond-to-putins-hybrid-warlatvia-estonia-lithuania-finland/

16. Understanding the Role of Hybrid Warfare and U.S. Strategy for Future Conflicts; 20170423; Center for International Maritime Security (CIMSEC) http://cimsec.org/understanding-role-hybrid-warfare-u-s-strategy-future-conflicts/32171

17. Hybrid Threats and Strengthening Resilience on Europe's Eastern Flank; 201703; George C. Marshall European Center for Security Studies; Dr. Pal Dunay, Professor of NATO and European Security Issues at the Marshall Center and Deputy Director of the ESS-E http://www.marshallcenter.org/MCPUBLICWEB/mcdocs/files/College/F_Publications/secInsights/security_insights_16.pdf

18. A Missing Shade of Gray: Political Will and Waging Something Short of War; 20170111; War On The Rocks, Phillip Lohaus, Research Fellow in the Marilyn Ware Center for Security Studies at the American Enterprise Institute, previously served as an associate with the Long Term Strategy Group and as an intelligence analyst with the U.S. Department of Defense. https://warontherocks.com/2017/01/a-missing-shade-of-gray-political-will-and-waging-something-short-of-war/

19. NATO Projecting Stability, 2017, Atlantic Treaty Association (ATA) (this is a compilation of approximately 20 articles related to the challenges faced by NATO from hybrid threats) http://issuu.com/globalmediapartners/docs/nato_projecting_stability?e=25557842%2F54244345

20. Developing Key Competencies in the RSAF to Defend against Hybrid Warfare; 2017; Pointer Journal, Singapore Air Force (RSAF) https://www.mindef.gov.sg/oms/safti/pointer/documents/pdf/V43N1a4.pdf

21. Five Steps the US Army Should Take to Counter Hybrid Threats in the Gray Zone, 20161020, West Point, Modern War Institute https://mwi.usma.edu/five-steps-us-army-take-counter-hybrid-threats-gray-zone/

22. Policy Brief: Local Capacity is the First Line of Defense Against the Hybrid Threat, 20150914, The German Marshall Fund of the United States http://www.gmfus.org/publications/local-capacity-first-line-defense-against-hybrid-threat

23. Assessing Canada's Integrated National Security Enforcement Teams: Can the Concept of INSETs Be Exported?; 201608; Global Education Community Collaboration Online (Global ECCO), Michael Turney, University of Waterloo https://globalecco.org/assessing-canada

24. Legal Aspects of Hybrid Warfare, 20151002; LAWFARE; Aurel Sari, Senior Lecturer in Law, University of Exeter and Director, Exeter Centre for International Law and Fellow,

Allied Rapid Reaction Corps; Arnis Lauva, Third Secretary, Legal Department of the Ministry of Foreign Affairs, Latvia
https://www.lawfareblog.com/legal-aspects-hybrid-warfare

25. Nonviolent Civilian Defense to Counter Russian Hybrid Warfare; 201503 ; Maciej Bartkowski, Ph.D., Johns Hopkins University
http://advanced.jhu.edu/academics/graduate-degree-programs/global-security-studies/program-resources/publications/white-paper-maciej-bartkowski/
26. Strategic Futures and Intelligence: The Head and Heart of 'Hybrid Defence' Providing Tangible Meaning and Ways Forward; Small Wars Journal, Adam D.M. Svendsen, PhD, (Warwick, UK), international intelligence and defense strategist and researcher
http://smallwarsjournal.com/jrnl/art/strategic-futures-and-intelligence-the-head-and-heart-of-%E2%80%98hybrid-defence%E2%80%99-providing-tangibl

REFERENCES

1. Hybrid CoE. The European Centre of Excellence for Countering Hybrid Threats. "Establishment." https://www.hybridcoe.fi/establishment/, accessed 18 August 2021.

2. Hybrid CoE. The European Centre of Excellence for Countering Hybrid Threats. "What is Hybrid CoE?" https://www.hybridcoe.fi/who-what-and-how/, accessed 18 August 2021.

3. Hybrid CoE. The European Centre of Excellence for Countering Hybrid Threats. "Hybrid Threats." https://www.hybridcoe.fi/hybrid-threats/, accessed 18 August 2021.

BIOGRAPHIES

Scott Armistead is a DSIAC SME who currently works as the DSIAC Senior Staff Engineer. Mr. Armistead served as a Test Engineer, Program Engineer, and Technical Advisor in the DoD and as a Test Manager for the Joint Munitions Test & Evaluation Program Office. He has nearly 35 years of experience in developmental, Live Fire, and operational research, development, test, and evaluation of DoD munitions, weapon systems, and platforms to include both kinetic and nonkinetic effects as well as development of planning and execution methodologies and documentation; modeling, simulation, and analysis tools; and forensics instrumentation, software, and techniques to support these efforts. He has supported numerous General Officer Steering Committees and command-level Joint and Tri-Service Red Teams, Integrated Product Teams, Working Groups, and roadmap development efforts. Mr. Armistead received his B.A. in Nuclear Engineering from the University of Florida.

Dominic Ju is a DSIAC SME and Marine Corps veteran who has been serving the military and commercial markets and academia since 2000. Mr. Ju currently is the Managing Principal and Co-Founder of BluePath Labs, an IAC support teammate. He has supported clients across the DoD, Intelligence Community (IC), and civilian agencies such as the Army TechWargaming program, Special Operations Command (SOCOM), Army Rapid Equipping Force (REF), Defense Intelligence Agency (DIA), multiple combatant commands (COCOMs), and the National Science Foundation (NSF). Mr. Ju also has experience working with Special Operations Forces. He has led civil-military teams to evaluate strategic plans and business processes, identify requirements, and assess risks for acquisition programs valued in excess of $2B USD to align emerging strategic initiatives with budgetary and fiscal realities. Mr. Ju received his B.A. from Tufts University and M.A. from the Fletcher School of Law and Diplomacy at Tufts University.

APPENDIX A: Hybrid Threats and Warfare Documents and Articles

Guides, Journal Articles, Papers, Regulations, and Reports Related to Hybrid Threats and Warfare

1. A 'Hybrid Threat'? European Militaries and Migration, 20180425, Dahrendorf Forum https://www.stiftung-mercator.de/media/downloads/3_Publikationen/2018/April/Militarising-Migration-Julia-Himmrich.pdf
2. Countering Russia's Hybrid Threats: An Update, 20180327, NATO Parliamentary Assembly, Committee on the Civil Dimension of Security https://www.nato-pa.int/download-file?filename=sites/default/files/2018-04/2018%20-%20COUNTERING%20RUSSIA'S%20HYBRID%20THREATS%20-%20DRAFT%20SPRING%20REPORT%20JOPLING%20-%20061%20CDS%2018%20E.pdf
3. Violence in Context: Mapping the Strategies and Operational Art of Irregular Warfare, 20180209, College of International Security Affairs, National Defense University https://www.tandfonline.com/doi/full/10.1080/13523260.2018.1432922?scroll=top&needAccess=true
4. Violent Non-State Actors and Contested Space Operations, 201802; Department of Homeland Security, National Consortium for the Study of Terrorism and Responses to Terrorism (The Violent Non-State Actors and Contested Space Operations project seeks to assess the risks posed by violent non-state actors to space-based systems. Moreover, it endeavors to also develop potential responses aimed at building resilience and countering threats.) http://www.start.umd.edu/research-projects/violent-non-state-actors-and-contested-space-operations (As of this TI response, the report was not currently posted, but should be soon; it can be requested through DSIAC.)
5. Russian Hybrid Tactics in Georgia; 201801; Central Asia-Caucasus Institute & Silk Road Studies Program https://silkroadstudies.org/resources/pdf/SilkRoadPapers/2018_01_Nilsson_Hybrid.pdf
6. Avoiding U.S.-Russia Military Escalation During the Hybrid War; 201801; Carnegie Endowment for International Peace, Dmitri Trenin, Director CEIP and Chair of the Foreign and Security Policy Program https://carnegieendowment.org/files/Trenin_Hybrid_War_web.pdf

7. "Sea of Peace" or Sea of War—Russian Maritime Hybrid Warfare in the Baltic Sea; 2018; U.S. Naval War College http://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1738&context=nwc-review
8. Transformation and the War in Afghanistan; 2018; Air University, Strategic Studies Quarterly; Alexander Salt, Ph.D. Candidate, University of Calgary, Centre for Military, Security and Strategic Studies http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-12_Issue-1/Salt.pdf
9. NATO LibGuide, Essentials of Hybrid Warfare, NATO http://www.natolibguides.info/hybridwarfare
10. Russian Hybrid Threats to the Baltic States; 20170712; The Polish Institute of International Affairs https://www.pism.pl/files/?id_plik=23368
11. Hybrid Threats and Asymmetric Warfare: What to Do?, 20171114, Swedish Defence University http://fhs.diva-portal.org/smash/get/diva2:1186265/FULLTEXT01.pdf
12. Future War NATO?: From Hybrid War to Hyper War via Cyber War; 201710; GLOBSEC NATO Adaptation Initiative https://www.globsec.org/wp-content/uploads/2017/10/GNAI-Future-War-NATO-JLF-et-al.pdf
13. Adapting CT Strategies to Combat Organized Crime Gangs; 201705; Global Education Community Collaboration Online (Global ECCO), Maj. Anders Westberg, Special Operations Command, Sweden https://globalecco.org/documents/10180/768889/CTX71-Adapting-CT-Strategies-to-Combat-Organized-Crime-Gangs/5e3f709a-3ae6-43ea-9dfd-4d7ecb92f960
14. Hybrid Warfare in the Baltics: Threats and Potential Responses, 2017, RAND Corp https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1577/RAND_RR1577.pdf
15. "Hybrid Warfare" – The Military Security Domain's Considerations; 2017; Estonian Journal of Military Studies, Estonian National Defense College http://www.ksk.edu.ee/wp-content/uploads/2017/08/Hybrid-warfare-the-military-security-domain%C2%B4s-considerations.pdf
16. Against the Ascent of Hybrid Warfare: Expanding the RSAF's Capacity in Peace and War; 2017; Pointer Journal, Singapore Air Force (RSAF) https://www.mindef.gov.sg/oms/safti/pointer/documents/pdf/V43N1a1.pdf

17. Technologies in Hybrid Warfare: Challenges and Opportunities; 2017; Pointer Journal, Singapore Air Force (RSAF) https://www.mindef.gov.sg/oms/safti/pointer/documents/pdf/V43N1a2.pdf

18. Cyber Threats in Hybrid Warfare: Securing the Cyber Space for the RSAF; 2017; Pointer Journal, Singapore Air Force (RSAF) https://www.mindef.gov.sg/oms/safti/pointer/documents/pdf/V43N1a3.pdf

19. NS50: Defending Singapore 50 Years and Beyond; 2017; Pointer Journal, Singapore Air Force (RSAF) https://www.mindef.gov.sg/oms/safti/pointer/documents/pdf/V43N1a5.pdf

20. Russian New Generation Warfare Handbook; 2017; US Army Asymmetric Warfare Group https://info.publicintelligence.net/AWG-RussianNewWarfareHandbook.pdf

21. Hybrid Warfare An Evolving Threat; 2017; Jane's HIS http://www.janes.com/images/assets/614/70614/Hybrid_warfare_An_evolving_threat.pdf

22. CTX Journal v6 n4, Special Edition: Hybrid Warfare; 201611; Global Education Community Collaboration Online (Global ECCO) https://globalecco.org/documents/327413/327631/Vol+6+No+4.pdf/

23. Outplayed: Regaining Strategic Initiative in the Gray Zone; 201606; Strategic Studies Institute and U.S. Army War College https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1325

24. Back to Basics on Hybrid Warfare in Europe: A Lesson from the Balkans; 20160329; National Defense University Press, Joint Force Quarterly 81; Dr. Christopher J. Lamb, Director, Center for Strategic Research, Institute for National Strategic Studies (INSS), National Defense University; Susan Stipanovich, Program Manager, Program on Irregular Warfare and Special Operations Studies at INSS http://ndupress.ndu.edu/Publications/Article/702045/back-to-basics-on-hybrid-warfare-in-europe-a-lesson-from-the-balkans/

25. Hybrid Wars: The 21st-Century's New Threats to Global Peace and Security; c2016; Sascha-Dominik Bachmann, Bournemouth University, UK and Håkan Gunneriusson, Swedish Defence University https://www.ajol.info/index.php/smsajms/article/viewFile/117421/106983

26. A Warning from the Crimea: Hybrid Warfare and the Challenge for the ADF; 201511; Capt Nicholas Barber, Intelligence Officer, 1st Intelligence Battalion, Australian Army http://www.defence.gov.au/adc/adfj/Documents/issue_198/Barber_Nov_2015.pdf

27. How Can Societies be Defended Against Hybrid Threats? 201509, Geneva Centre for Security Policy

http://www.defenddemocracy.org/content/uploads/documents/GCSP_Strategic_Security_Analysis_-_How_can_Societies_be_Defended_against_Hybrid_Threats.pdf

28. A Closer Look at Russia's "Hybrid War"; 201504; Wilson Center Kennan Institute https://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf
29. Russia's Hybrid Warfare: Waging War Below the Radar of Traditional Collective Defense; 201411; NATO OTAN, ETHzurich, Center for Security Studies https://www.files.ethz.ch/isn/185744/rp_105.pdf

Web Articles Related to Hybrid Threats and Warfare

1. NATO Countering the Hybrid Threat, 20110912, NATO OTAN & National Defence University http://www.act.nato.int/nato-countering-the-hybrid-threat
2. 'Hybrid Threat'?: Defining Russian Intelligence Strategy, 20180404, Grey Dynamics https://www.greydynamics.com/single-post/2018/04/04/%E2%80%98Hybrid-threat%E2%80%99-Defining-Russian-Intelligence-Strategy
3. What is Hybrid Warfare?, 20180415, Global Security https://globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/
4. Cross Domain Concerns: Defeating a Hybrid State's Grand Strategy, 20180222, RealClear Defense https://www.realcleardefense.com/articles/2018/02/22/defeating_a_hybrid_states_grand_strategy_113097.html
5. Hybrid Warfare and Hybrid Threats, 20180416, European Eye on Radicalization https://eeradicalization.com/hybrid-warfare-and-hybrid-threats/
6. Europe and U.S. Move to Fight Russian Hybrid Warfare; 20170411; The Diplomat, Reid Standish and Emily Tamkin http://foreignpolicy.com/2017/04/11/europe-and-u-s-move-to-fight-russian-hybrid-warfare/
7. The Perils of Hybrid War, 201704, Air Force Magazine http://www.airforcemag.com/MagazineArchive/Pages/2017/March%202017/The-Perils-of-Hybrid-War.aspx
8. Marshall Center European Security Seminar Explores Hybrid Threats, Resilience Building, 20170131, U.S. Army

https://www.army.mil/article/181628/marshall_center_european_security_seminar_explores_hybrid_threats_resilience_building

9. Hybrid Threats from the East: The Gerasimov Doctrine and Intelligence Challenges for NATO, 20170922, Militaire Spectator http://www.militairespectator.nl/thema/strategie/artikel/hybrid-threats-east
10. Avoiding U.S.-Russia Military Escalation During the Hybrid War, 20180125, Carnegie Moscow Center http://carnegie.ru/2018/01/25/avoiding-u.s.-russia-military-escalation-during-hybrid-war-pub-75277
11. The Islamic State is a Hybrid Threat: Why Does That Matter?, 2014, Small Wars Journal, Center for Civil-Military Relations at the Naval Postgraduate School and National Security Affairs Department at the Naval Postgraduate School http://smallwarsjournal.com/jrnl/art/the-islamic-state-is-a-hybrid-threat-why-does-that-matter
12. Hybrid War: Attacking The 'Civil' In Civil Society, 20180413, U.S. Army War College, War Room https://warroom.armywarcollege.edu/articles/hybrid-war-attacking-the-civil-in-civil-society/
13. Responding to Russia's 'Hybrid' Threat: 6 Ways the EU and NATO can Head Off Russia's Many-Pronged Attack on Western Democracy, 20170424, US News https://www.usnews.com/opinion/world-report/articles/2017-04-24/6-ways-the-us-eu-and-nato-can-meet-and-defeat-russias-hybrid-threat
14. State and Non-State Hybrid Warfare, 20170330, Oxford Research Group Sustainable Security Programme https://sustainablesecurity.org/2017/03/30/state-and-non-state-hybrid-warfare/
15. The West Attempts Hybrid Resistance, 20170807, Matthias Monroy, Editor, Bürgerrechte & Polizei/CILIP (German civil rights journal) https://digit.site36.net/2017/08/07/the-west-attempts-hybrid-resistance/
16. Putin's Postmodern War with the West, 2018, The Wilson Quarterly, Patryk Babiracki, Professor Russian and East European History, University of Texas at Arlington, former Title VIII researcher at Wilson Center's Kennan Institute https://www.wilsonquarterly.com/quarterly/the-disinformation-age/putins-postmodern-war-with-the-west/
17. China's Hybrid Warfare and Taiwan: How China Could Use "Fake News" and Digital Warfare in Its Preparations for Engagement with Taiwan, 20180113, The Diplomat https://thediplomat.com/2018/01/chinas-hybrid-warfare-and-taiwan/

18. Hybrid Warriors: China's Unmanned, Guerrilla-Style Warfare in Asia's Littorals; 20170216; The Diplomat https://thediplomat.com/2017/02/hybrid-warriors-chinas-unmanned-guerilla-style-warfare-in-asias-littorals/

19. Hybrid War – Does It Even Exist?, 2015, NATO OTAN, NATO Review https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0ahUKEwjm85Dw58HbAhVCaq0KHfh4A14QFgg-MAQ&url=https%3A%2F%2Fwww.nato.int%2Fdocu%2Freview%2F2015%2Falso-in-2015%2Fhybrid-modern-future-warfare-russia-ukraine%2Fen%2Findex.htm&usg=AOvVaw0psXu4pViyf-cavxxw5HGj

20. Special Issue: The Evolving Threat of Hybrid War, 20170912; Bulletin of the Atomic Scientists https://thebulletin.org/press-release/special-issue-evolving-threat-hybrid-war11101

21. Predicting Future Trends in Warfare; 20180221; King's College London, Defence Studies Department https://defenceindepth.co/2018/02/21/predicting-future-trends-in-warfare/

22. Current Russian and Chinese Ways of Warfare: The End (?) of Military Violence in Peer-State Conflict; 20180117; King's College London, Defence Studies Department https://defenceindepth.co/2018/01/17/current-russian-and-chinese-ways-of-warfare-the-end-of-military-violence-in-peer-state-conflict/

23. The Ukrainian Crisis: The Role of, and Implications for, Sub-State and Non-State Actors; 20170628; King's College London, Defence Studies Department https://defenceindepth.co/2017/06/28/the-ukrainian-crisis-the-role-of-and-implications-for-sub-state-and-non-state-actors/

24. Hybrid War: The Perfect Enemy; 20170425; King's College London, Defence Studies Department https://defenceindepth.co/2017/04/25/hybrid-war-the-perfect-enemy/

25. The Russian Military's View On the Utility of Force: The Adoption of a Strategy of Non-Violent Asymmetric Warfare; 20170217; King's College London, Defence Studies Department https://defenceindepth.co/2017/02/17/the-russian-militarys-view-on-the-utility-of-force-the-adoption-of-a-strategy-of-non-violent-asymmetric-warfare/

26. Russia's Hybrid Warfare: Waging War Below the Radar of Traditional Collective Defense; 201411; NATO OTAN, ETHzurich, Center for Security Studies https://www.files.ethz.ch/isn/185744/rp_105.pdf

27. Special Report, Shades of Grey: Neither War nor Peace – The Uses of Constructive Ambiguity; 20180125; The Economist https://www.economist.com/special-report/2018/01/25/neither-war-nor-peace

28. Hybrid Warfare Revisited; 201505; Global Education Community Collaboration Online (Global ECCO), LTC Fabian Sandoris, Special Forces, Hungarian Army https://globalecco.org/hybrid-warfare-revisited

29. Lithuanian Social Resilience in the Face of Russia's Unconventional Hostility; 20180419; The Jamestown Foundation, Dr. Dainius Genys, Andrei Sakharov Research Center for Democratic Development, Vytautas Magnus University, Kaunas https://jamestown.org/analyst/dainius-genys/

30. Preparing for the Worst: Poland's Military Modernization; 20180322; Foreign Policy Research Institute, Felix K. Chang, Senior Fellow, Foreign Policy Research Institute and CSO, DecisionQ (national security and healthcare predictive analytic) https://www.fpri.org/2018/03/preparing-for-the-worst-polands-military-modernization/

31. Cold War 2.0 – Part 1: The Protagonists of a New Conflict; 20180303; The Foreign Analyst http://theforeignanalyst.com/cold-war-2-0-part-1-the-protagonists-of-a-new-conflict/

32. Cold War 2.0 – Part 2: Russia's Hybrid Warfare; 20180306; The Foreign Analyst http://theforeignanalyst.com/cold-war-2-0-part-2-russias-hybrid-warfare/

33. Hybrid War in The Western Hemisphere; 20170604; Geopolitica (Russian website) https://www.geopolitica.ru/en/article/hybrid-war-western-hemisphere

34. Nationalism: Russian Hybrid Warfare; 20170218; International Policy Digest, Cynthia Lardner https://intpolicydigest.org/2017/02/18/nationalism-russian-hybrid-warfare/

35. Hybrid Warfare in the South China Sea: The United States' 'Little Grey (Un)Men'; 20161231; The Diplomat, Tobias Burgers and Scott Romaniuk https://thediplomat.com/2016/12/hybrid-warfare-in-the-south-china-sea-the-united-states-little-grey-unmen/

36. Hybrid Threats 2016; 201512; Dr Sascha-Dominik Oliver Vladimir Bachmann, Bournemouth University https://www.researchgate.net/publication/292132828_HYBRID_THREATS_2016

Other Materials Related to Hybrid Threats and Warfare

1. SMARTbooks – Threat, OPFOR, Regional & Cultural Set
   - CTS1: The Counterterrorism, WMD & Hybrid Threat SMARTbook
   - TAA2: The Military Engagement, Security Cooperation & Stability SMARTbook, 2nd Ed. (w/Change 1)
   - OPFOR SMARTbook 3 – Red Team Army
   - Cultural Guide SMARTbook 1 – Afghanistan
   - HDS1: The Homeland Defense & DSCA SMARTbook
   https://www.thelightningpress.com/opposing-forces/