The Use of Cyberspace in the Context of Hybrid Warfare: Means, Challenges and Trends

Abdyraeva, Cholpon

Veröffentlichungsversion / Published Version
Arbeitspapier / working paper

Working Paper
107/ June 2020

Österreichisches Institut
für Internationale Politik
Austrian Institute for
International Affairs

The Use of Cyberspace in the Context of Hybrid Warfare. Means, Challenges and Trends

Cholpon Abdyraeva

Working Paper 107 / June 2020

Keywords:
hybrid warfare, cyberspace, cyber warfare, Russia

Cholpon Abdyraeva, MSc studies Political Science (MA) at the University of Vienna with a focus on Cyber Security und Foreign Policy Analysis. She is an intern at the Austrian Institute for International Affairs and is a part of terrorism/ political violence team. Her specific research interests lie in the areas of anti-terrorism cooperation, democratization and studies of social movements.

Impressum:

Österreichisches Institut für Internationale Politik – oiip,
1090 Wien, Berggasse 7, www.oiip.ac.at, info@oiip.ac.at

Die wichtigsten Erkenntnisse auf Deutsch:

Die Nutzung des Cyberraums im Kontext der hybriden Kriegsführung.

Mittel, Herausforderungen und Trends

Der vorliegende Artikel zielt darauf ab, den neuesten Forschungsstand in Bezug auf hybride Kriegsführung zu veranschaulichen und die konzeptionelle Verwirrung hinsichtlich eines ständig wachsenden Konzepts der hybriden Kriegsführung anzugehen. Auf diese Weise wird gleichzeitig versucht, die wachsende Bedeutung des Cyber- und Informationsraums innerhalb der hybriden Kriegsführung aufzuzeigen, was vor allem am Beispiel der russischen hybriden Kriegsführung veranschaulicht werden kann. So hat der russische Ansatz den Umfang der hybriden Kriegsführung erheblich erweitert und den Schwerpunkt der Debatten von militärischen auf nicht-militärische Komponenten der hybriden Kriegsführung verlagert. Aus diesem Grund dient der vorliegende Artikel zwei Zwecken: 1) ein tieferer Einblick in die hybride Kriegsführung inklusive der darin vorhandenen Trends 2) Analyse der Rolle bzw. Auswirkungen des Cyber- und Informationskriegs mit besonderem Schwerpunkt auf Russland. Der Artikel ist wie folgt strukturiert: Nach einer Einführung in die hybride Kriegsführung in Kapitel 2, untersucht Kapitel 3 die Nutzung des Cyberraums im Kontext der hybriden Kriegsführung, liefert Gründe dafür, warum Staaten im Cyberraum Krieg führen (3.1) und untersucht die Trends im Cyberkrieg (3.2). Im empirischen Teil (Kapitel 4) wird eine Analyse des Informationskriegs durchgeführt mit besonderem Fokus auf russische Informationsoperationen im Cyber-Domain. Der Artikel kann politischen Entscheidungsträgern einen Einblick in das Thema bzw. in Expertenmeinungen geben und als Anregung für weitere Untersuchungen in diesem Bereich dienen.

Die hybride Kriegsführung ist eine Mischung aus konventioneller und unkonventioneller Kriegsführung, die gleichzeitig den Einsatz „konventioneller Fähigkeiten, irregulärer Taktiken und Formationen sowie terroristischer Handlungen wie wahllose Gewalt, Zwang und kriminelle Aktivitäten“ kombiniert (Hoffman, 2007, S. 8). Hybride Kriegsführung verbindet mehrere Werkzeuge untereinander und findet auf mehreren „Schlachtfeldern“ gleichzeitig statt, was die Reaktion darauf komplexer und schwieriger gestaltet. Die Machtinstrumente, die ein hybrider Akteur gegen die Schwachstellen eines Gegners einsetzen kann, sind stark kontextabhängig. Eine zentrale Idee der hybriden Kriegsführung ist die Verwendung von sozialen Medien als „Waffe“. Die von Staaten mit *munitionierten* Informationen verbreiteten Online-Geschichten liefern sich gegenseitig schnelle Schlagabtäusche und eine Intensivierung des Diskurses, was von den UserInnen der sozialen Medien kaum zu übersehen ist. So wird in Sekundenschnelle ein globales Publikum bei minimalen Kosten erreicht.

Cyberkrieg

Neben den drei Schlachtfeldern der hybriden Kriegsführung - konventionelles Schlachtfeld, die in einen Konflikt geratene indigene Bevölkerung und die internationale Gemeinschaft (McCuen, 2008, S.107) – wird nun auch der Cyberraum als neues Schlachtfeld für den Wettbewerb zwischen Staaten offiziell anerkannt. Die Cyberkriegsführung hat sich zu einer zusätzlichen Herausforderung für die internationale und nationale Sicherheit entwickelt.

Der Aufstieg des Cyberbereichs als neue strategische Herausforderung

Im Vergleich zu konventionellen Kriegen sind Cyberoperationen relativ günstig durchzuführen und sowohl für Staaten als auch für nichtstaatliche Akteure leicht zugänglich. Darüber hinaus können sie eine größere Wirkung erzielen und bieten die Möglichkeit, einen Krieg ohne physische Konfrontation sowie einer Kriegserklärung zu führen. Die Identifizierung bzw. Ausforschung von Beteiligten eines Cyberangriffes gestaltet sich als äußerst schwierig, wobei auch rechtliche Belange aufgrund fehlender Beweise bzw. internationalen Rechtsrahmen kaum möglich sind (Grisby, 2017; Georgieva, 2020). Die größte Herausforderung für Cyberwaffen und Cyberoperationen besteht darin, dass nicht sicher ist, ob die Akteure den Cyberraum für Angriffs- oder Verteidigungszwecke nutzen. Darüber hinaus besteht Unsicherheit über die Reaktion des Ziellandes oder der internationalen Gemeinschaft auf Cyberangriffe. Die strategischen Vorteile von Cyberwaffen ist für viele Staaten der Grund für einen Ausbau der Cyberfähigkeiten. Neben der Entwicklung von Cyberprogrammen und Einsatzregeln für die Nutzung des Cyberraums, sind die Bereiche Cyberraum und IT-Sektor schnellen Veränderungen unterworfen, weshalb sie immer komplexer und hochentwickelter werden. Aus diesem Grund ist man sich weitgehend einig, dass cyberfähige Technologien zwangsläufig zu einer Veränderung des internationalen und nationalen Sicherheitsumfelds führen werden.

Arten von Cyberangriffen und Trends in der Cyber-Kriegsführung

Heutzutage sind Cyberangriffe aufgrund ihrer zunehmenden Raffinesse und Häufigkeit öfters ein internationales Problem. Dies ist wiederum das Ergebnis der Entwicklung von Angriffstechnologien, des Auftretens staatlich geförderter Cyberkampagnen gegen Regierungseinheiten und einer stärkeren Vernetzung zwischen Hackern. Dadurch wurden Cyberbedrohungen „allgegenwärtiger“ und schwerwiegender. Mittels Stärkung ihrer Cybermacht versuchen immer mehr Staaten durch Cyberkriegsführung ihre politischen Ziele, die außerhalb des Cyberbereichs liegen, zu erreichen. Denn die Machtverteilung zwischen Staaten kann durch Cyberkriegsführung erheblich beeinflusst werden, ohne eine direkte militärische Konfrontation zu provozieren (Dunn Cavelty und Wenger, 2020, S. 12).

Die Aktionen nationalstaatlicher Akteure im Cyberbereich haben zu einer Erweiterung des Umfangs der Cyberangriffe geführt. Zum einen gibt es nichtstaatliche und staatlich geförderte Akteure, die strategische Cyberangriffe gegen kritische Infrastruktureinheiten durchführen. Sie hacken sich in Unternehmensnetzwerke, um Informationen über bestimmte Personen zu stehlen oder Viren bzw. Spyware zu installieren. Zum anderen führen staatlich geförderte Operationen einen Informationskrieg im Cyberbereich, indem Datenmanipulationsangriffe eingesetzt werden, um u.a. die öffentliche Meinung absichtlich zu beeinflussen. Dabei erstellen Trolle und Bots Online-Inhalte und Verbreiten Fehlinformationen.

Cyberwaffen werden als Zwangsmittel eingesetzt und decken einen weiten Bereich der Schadensaktivitäten von staatlichen und nichtstaatlichen Akteuren ab (Claver, 2018, S. 158). Cyberangriffe können einerseits in „syntaktische Angriffe“ - die über bösartige Software bzw. Viren und Würmen die Benutzer angreift - unterteilt werden, andererseits in "semantische Angriffe". Diese zielen auf Infrastrukturen oder IT-Einrichtungen ab und nehmen Datenänderungen - z.B. Phishing und Malvertising - unbemerkt vor (Knopová und Knopová, 2014, S. 25-26).

Darüber hinaus gibt es einen alarmierenden Trend zur Spionage durch staatlich geförderte Cybergruppen. Tabelle 1 bietet einen detaillierten Überblick über diesen Trend, dessen Grundlage sich auf die Ergebnisse der von Osawa (2017) vorgelegten Forschungsanalyse bezieht. Bis 2018 gab es ingesamt 41 mit der russischen, chinesischen, iranischen und nordkoreanischen Regierungen assoziierten Personen, die angeblich an staatlich geförderter Spionage gegen die Vereinigten Staaten beteiligt waren. Ziel der Angriffe waren Regierungsbehörden, Banken, das Gesundheitswesen, internationale Organisationen und Unternehmen, womit die jeweiligen politischen Ziele der Angriffsländer erreicht werden sollen. (Kiefer et al., 2019)

Table 1. Major State-sponsored Cyber Attacks (2007-2017)

(Year/Month)
- 2007.4 Estonia; cyber sabotage targeting government, media, financial sector.
- 2008.7 Lithuania; cyber sabotage targeting government, private sector.
- 2008 U.S. DoD; cyber intrusion and espionage.
- 2008.8 Georgia; cyber sabotage targeting government, media, financial sector.
- 2009.1 Kyrgyzstan; cyber sabotage targeting Internet Service Providers.
- 2009.7 ROK and U.S.; cyber sabotage targeting government.
- 2009.12 Google, cyber intrusion on its core system. Google retreated from business in China.
- 2010.8 Iran; Stuxnet, cyber subversion targeting Iranian uranium-enrichment plant.
- 2011.9 Japan; cyber espionage targeting defense industry, including MHI and IHI.
- 2011.10 Japan; cyber espionage targeting parliament member.
- 2011–12 U.S.; Iranian state-sponsored actor conducted cyber sabotage against financial sector.
- 2012.8 Saudi Arabia and Quarter; cyber subversion targeting energy industry, Saudi Aramco, RasGas.
- 2012.12–13.1 U.S.; cyber espionage targeting major newspapers and think tanks.
- 2013.3 ROK; cyber sabotage targeting media and financial sector.
- 2014.3 Ukraine; cyber sabotage targeting government and telecommunication company.
- 2014.5 Belgium; cyber espionage targeting Ministry of Foreign Affairs
  cf. 2010- European countries; cyber espionage targeting government, int'l organization.
- 2014.8 U.S.; cyber intrusion and financial cyber crimes targeting JP Morgan, etc.
- 2014.10 U.S.; cyber intrusion and espionage targeting White House and State Department.
- 2014.11 U.S.; cyber subversion targeting Sony Pictures Entertainment. U.S. government identified the attacking group and sanctioned North Korea (the first attributed state-sponsored attack).
- 2015.4 France; cyber subversion targeting TV5.
- 2015.4 U.S.; cyber intrusion and espionage targeting U.S. Office of Personnel Management, resulted in the theft of sensitive information of 21.5 million individuals.
- 2015 Germany; cyber espionage targeting Germany. Germany BND accused Russia.
- 2015.5 Japan; cyber espionage targeting Pension Service, 1.25 million records breached.
- 2015.12 Ukraine; cyber subversion targeting power grid company. (the first officially attributed state-sponsored attack on Critical Infrastructure)
- 2016.2 Bangladesh; cyber theft targeting the central bank, $81 million stolen.
- 2016.3 Sweden; cyber sabotage targeting media sector.
- 2016.4 Lithuania; cyber sabotage targeting its parliament.
- 2016.8 Viet Nam; cyber sabotage targeting international airports.
- 2016.11 Saudi Arabia; cyber subversion targeting government and private sector.
- 2016.11 U.S.; Russian cyber intrusion and espionage targeting Democratic National Committee.
- 2016.12 Ukraine; cyber subversion targeting power grid company in Kiev.
- 2017.4 Japan; new style cyber espionage operation named "Cloud Hopper" by APT10.
- 2017.5 World-wide; cyber subversion by the Wannacry ransomware cyber pandemic.
- 2017.6 World-wide; cyber subversion by the Petya/Not-Petya ransomeware cyber pandemic.

Source: Author, using open source materials.

Osawa (2017) argumentiert, dass ein übergeordneter Trend zu staatlich geförderten Cyberangriffen durch die Tatsache erklärt werden kann, dass diese Angriffe „häufig auf Vorfälle internationaler Zwietracht oder Konflikte zurückzuführen sind" (S. 115). So wurde insbesondere die Annexion der Krim im Jahr 2014 zum Schwerpunkt des erneuten Konflikts zwischen Russland und den USA. Seitdem wurden Russland umfangreiche Cyberangriffe gegen die USA sowie gegen die Ukraine und den NATO-Mitgliedstaaten vorgeworfen. Am bekanntesten sind die Versuche Russlands, Zugang zu den kritischen Infrastrukturen und Wahlsystemen in der Ukraine zu erlangen. Laut dem Bericht der Internationalen Stiftung für Wahlsysteme haben angeblich russische Hacker einige Tage vor der Präsidentschaftswahl 2014 einen Cyberangriff auf die Zentrale Wahlkommission der Ukraine gestartet, um das Ergebnis der Wahl zu beeinflussen.

Die wachsende Bedeutung des „Dark Web" und die daraus entstehenden Möglichkeiten sind ein weiterer aufkommender Trend in der Cyberkriegsführung. Das „Dark Web" trägt einerseits zum An-

stieg von Cyberangriffen bei, da es kriminellen Gruppen und Terroristen die Möglichkeit bietet, unentdeckt und somit ungestraft zu bleiben. Andererseits fördert das „Dark Web" die Professionalisierung der Hacking-Methoden und -Techniken von Cybergruppen durch Diskussionsforen und dem Zugang zu den neuesten Hacking-Tools.

Informationskrieg der russischen Regierung im Cyber-Raum: Eine Fallstudie

Der Informationskrieg wird allgemein als ein breites und umfassendes Konzept angesehen, welches eine Reihe feindlicher Operationen abdeckt, indem Informationen als „Werkzeug, Ziel oder Operationsbereich" verwendet werden (Giles, 2016, S. 6). Die russische Regierung verfolgt jedoch einen ganzheitlichen Ansatz der Informationskriegsführung, der nicht nur „Auswirkungen hat auf den Zielstaat und die Fähigkeit seiner Streitkräfte hinsichtlich der Verwaltung von Informationen und der wirksamen Ausübung von Kommandos (…), sondern auch die Wahrnehmungen und Entscheidungsprozesse der Zielgruppen beeinflusst, um so die Interessen und Ziele Russlands zu fördern" (Tashev et al., 2019, S. 139). Anstatt Cyberoperationen im Rahmen der Cyberkriegsführung zu konzipieren, werden diese von der russischen Regierung in einen breiteren Rahmen der Informationskriegsführung eingegliedert. Dieser umfasst desinformative und psychologische Kampagnen, Cyberspionage sowie Cyberangriffe auf kritische Infrastruktureinrichtungen und wahlbezogene Technologien. Ein Beispiel für den hybriden Ansatz der russischen Kriegsführung ist ein auf die Ukraine entworfener Cyber-Angriffsplan, der vielfältige Aktivitäten wie Desinformation, den Einsatz von Stellvertretern und Aufständen sowie militärische Aktionen und wirtschaftliche Manipulationen kombiniert. Hacktivismus und Cyberkriminalität waren ein wichtiges Merkmal der offensiven Cyber- und Militäreinsätze von Russland im Ukraine-Konflikt. Zu den ukrainischen Cyberaktionen gehörten spezifische Angriffe von pro-Kiew Hackern, wie Anonymous Ukraine und Ukrainian Cyber Forces (UCFs), auf Kommunikations- und Privatunternehmen, wohingegen die pro-russischen Cyberakteure CyberBerkut, Green Dragon und Cyber Riot Novorossiya ukrainische Medien, Regierungsbeamte und Privatpersonen angriffen (Kostyuk und Zhukov, 2019, S. 324). Eine weitere Form der strategischen Informationskriegsführung sind Informationsmanipulationen, die z.B. die Narrative über den Ukraine-Konflikt *framten* bzw. beeinflussten. Dabei wurden unter den Zielgruppen pro-russische Einstellungen erzeugt und das Kampfpotential des Feindes erheblich verringert (vgl. Perry 2015).

Russischer Informationskrieg: Hacks und Leaks

Es gibt drei Arten von Instrumenten im Informationskrieg, die – so wird berichtet - von der russischen Regierung implementiert werden: 1) das Durchsickern persönlicher Informationen, 2) Hacking-Angriffe, u.a. die Erstellung automatisierter Benutzerkonten und Bots auf Social-Media-Plattformen wie Twitter, Facebook und YouTube, 3) die Verbreitung von Fake News und Verschwörungstheorien

über staatlich unterstützte Rundfunkanstalten. 2016 übernahm ein Hacker namens „Guccifer 2.0“, der sich als ein Offizier des russischen Militärgeheimdienstes (GRU) bezeichnete, die Verantwortung für den Hackerangriff auf das Netzwerk des Demokratischen Nationalkomitees und die Veröffentlichung der gestohlenen E-Mails und Dokumente der Demokratischen Partei auf WikiLeaks.

Russischer Informationskrieg: Verschwörungstheorien und Propaganda

IT-Technologie wie soziale Medien und das Internet erhöhen das Destabilisierungs- und Krisenbildungspotential des Informationskriegs erheblich, was möglicherweise dazu beitragen könnte, dass Staaten Auseinandersetzungen auf der psychologischen Ebene gewinnen, ohne überhaupt militärische Maßnahmen zu ergreifen (Lanoszka, 2019, S. 241). Die Verbreitung von Verschwörungstheorien durch die russische Regierung ist ein Beispiel für einen fortgeschrittenen Angriff des Informationskriegs im Cyberspace. Eine mehrmals formulierte Behauptung bezieht sich darauf, dass Russland angeblich einen Informationskrieg gegen die deutsche Bundeskanzlerin Angela Merkel geführt habe, was sich durch die erfundene Kampagne „Unsere Lisa“ geäußert hat. Darin wird für Unterstützung für ein minderjähriges russisch-deutsches Mädchen geworben, das angeblich von muslimischen Flüchtlingen entführt und vergewaltigt wurde, wie falsche Berichterstattungen behaupteten. Snyder (2018) argumentiert, dass diese Desinformationskampagne Angela Merkels Position in der Migrationspolitik geschwächt hat und infolgedessen ihre Zustimmungswerte unter den (sowohl deutschen als auch russisch-deutschen) Bürgern erheblich gesunken ist.

Literaturverzeichnis

Claver, A. (2018) "Governance of Cyber Warfare in the Netherlands: An Exploratory Investigation", *The International Journal of Intelligence, Security and Public Affairs* (20), pp. 155–180.

Dunn Cavelty M. and Wenger A. (2020) "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science", *Contemporary Security Policy* (41:1), pp. 5-32.

Georgieva I. (2020) "The Unexpected Norm-settlers: Intelligence Agencies in Cyber Space", *Contemporary Security Policy* (41), pp. 33-54.

Giles, K. (2016) "Handbook of Russian Information Warfare", NATO Defense College (9), pp. 1-78.

Grisby, A. (2017) "The End of Cyber Norm", *Survival* (59), pp. 109–122.

Hoffman, F. (2007) *Conflict in the 21st Century: The Rise of Hybrid War*. Arlington: Potomac Institute for Policy Studies.

Kiefer, K., Abbas, N., and Poole, E. (2019) "Cyber Alert: Ten Lessons from Six 2018 DOJ Indictments of State-Sponsored Hackers", *Alston & Bird*, 29 January, [Online] https://www.alston.com/en/insights/publications/2019/01/ten-lessons-from-six/ [Accessed: 05 May 2020].

Kostyuk, N. and Zhukov, Y. M. (2019) "Invisible Digital Front: Can Cyber Attacks Shape Batterfield Events?" *Journal of Conflict Resolution* (63:2), pp. 317-347.

Knopová, M. and Knopová *E*. (2014) "The Third War In The Cyberspace? Cyber Warfare in the Middle East", *Acta Informatica Pragensia* (3:1), pp. 23–32.

Lanoszka, A. (2019) "Disinformation in International Politics", *European Journal of International Security* (4), pp. 227 - 248.

McCuen, John J. "Hybrid Wars." Military Review. Mar/Apr 2008, Vol. 88 Issue 2, 107-113.

Osawa, J. (2017) "The Escalation of State Sponsored Cyberattack and Cyber Security Affairs: Is Strategic Cyber Deterrence The Key to Solving The Problem?" *Asia-Pacific Review* (24), pp. 113–131

Perry, B. (2015) "Non-Linear Warfare in Ukraine: The Critical Role of Information Operations And Special Operations", *Small War Journal*, 14 August, [Online] https://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera#_edn81 [Accessed: 24 May 2020].

Snyder, T. (2018) *The Road to Unfreedom: Russia, Europe, America* (New York: Tim Duggan Books.).

Tashev, B., Purcell, M. and McLaughlin, B. (2019) "Russia's Information Warfare. Exploring the Cognitive Dimension", *Marine Corps University Journal* (10:2), pp. 129-147.

Executive Summary

This paper aims to introduce the state of art on hybrid warfare and seeks to address the conceptual confusion regarding an ever-expanding concept of hybrid warfare. By doing so, this paper simultaneously attempts to assess the growing significance of cyber and information domains within the hybrid warfare, which can be clearly illustrated by the example of the Russian hybrid warfare strategy. The Russian approach to hybrid warfare has considerably broadened the scope of hybrid warfare and changed the focus of debates from military to non-military components of hybrid warfare. Therefore, the purpose of this paper is: 1) to produce a deeper insight into hybrid warfare, including related trends, and 2) to assess the role and impact of cyber and information warfare with a particular focus on Russia. Accordingly, this paper is structured as follows: following an introduction into hybrid warfare in Chapter 2, Chapter 3 explores the use of cyberspace within the context of hybrid warfare, provides reasons for why states conduct warfare in cyberspace (3.1) and explores the trends in cyber warfare (3.2). The empirical component starts with Chapter 4 that conducts an analysis of the information warfare and pays specific attention to the Russian cyber-enabled information operations. This paper can serve as an introduction that guides policy makers with expert opinions, and as such, intends to motivate further investigation in this field.

Table of Content

1. Introduction

The term and phenomenon of hybrid warfare are not new. The notion of hybrid warfare emerged in the period after the end of the Cold War but gained special prominence after the annexation of Crimea by the Russian Federation in 2014. Since then, the term of hybrid warfare became largely widespread and is now widely used as a "catch-all phrase or a buzzword" that captures a broad range of contemporary security and defense challenges (Reichborn-Kjennerud and Cullen, 2016, p.1). But despite the frequent use of the term by academics, media, military personnel and politicians, there is no commonly accepted definition of hybrid warfare (see *Figure* 1 for a list of definitions). Moreover, the meaning, the content and the usage of the term itself have experienced significant changes alongside a shift in the international security environment. For instance, in contrast to the newer definitions, the first definitions of hybrid warfare and hybrid threats were conceptualized within Western military circles in regard to the threats posed by the Taliban and Hezbollah in the context of Iran's operations against US forces 1987–88 during the Iran–Iraq War and Second Lebanon War in 2006, which implied the conflict between state and non-state actors. In this regard, it emphasized the acquisition of new techniques and sophisticated skills by non-state actors while simultaneously using conventional and unconventional means of warfare within the same battlespace.

As hybrid warfare became more widespread and the breadth of operations available to a hybrid warfare attacker substantially expanded, the term of hybrid warfare has attracted the attention of numerous researchers and policy makers, who undertook considerable conceptual alternations of hybrid warfare. The newer definitions of hybrid warfare tend now to neglect non-state actors and focus more on state actions, i.e. how state hybrid warfare strategically exploits the enemy's critical vulnerabilities across military, economic, social, cyber, and information management. The integration of cyber warfare tools and techniques to information warfare, in particular, has caused an open discussion about the conceptual stretching of hybrid warfare, as well as the conceptualisation of cyber and information warfare as both concepts overlap and twine together. Therefore, this paper aims to introduce the state of art on hybrid warfare and seeks to address the conceptual confusion regarding an ever-expanding concept of hybrid warfare.

By doing this, this paper simultaneously attempts to assess the growing significance of cyber and information domains within the hybrid warfare, which can be most visibly illustrated by the example of the Russian hybrid warfare strategy. The Russian approach to hybrid warfare has considerably broadened the scope of hybrid warfare and changed the focus of debates from military to non-military components of hybrid warfare. That is why this paper has two purposes: 1) to produce a

deeper insight into hybrid warfare, including trends within it, 2) to assess the role and impact of cyber and information warfare with a particular focus on Russia. Accordingly, this paper is structured as follows: following an introduction into hybrid warfare in Chapter 2, Chapter 3 explores the use of cyberspace within the context of hybrid warfare, provides reasons for why states conduct warfare in cyberspace (3.1) and explores the trends in cyber warfare (3.2). The empirical component starts with Chapter 4 that conducts an analysis of the information warfare and pays specific attention to the Russian cyber-enabled information operations. This paper can serve as an introduction that guides policy makers with expert opinions, and as such, intends to motivate further investigation in this field.

2. Hybrid Warfare: Trends, Challenges and Means

The majority of contemporary definitions of hybrid warfare try to capture the essence of hybrid warfare, however, in doing so, each definition mostly tries to explain the shifting meaning of 'hybrid warfare', which, in turn, further broadens its scope. Inevitably, as hybrid warfare has been increasingly used to describe both non-state and state-centric hybrid warfare, the concept of hybrid warfare became hazy, which, in turn, caused an open and heated scholarly debate on not only how to define hybrid warfare, but also whether the term is useful at all. Therefore, the main challenge of hybrid warfare lies in clarifying the concept in a way as "to make it useful" (Reichborn-Kjennerud and Cullen, 2016, p.1). In this regard, it is worth drawing attention to the explanatory weaknesses of definitions of hybrid warfare. For instance, the newer definitions of hybrid warfare do not specify whether non-military capabilities are used in order to avoid a military operation or rather serve as a precursor to a military campaign. Likewise, the newer definitions of hybrid warfare do not specify the role of the armed forces, as to whether the threat of using military serves as a mean to deter war or rather escalate the conflict. In contrast, most definitions of hybrid warfare tend to focus exclusively on two aspects – means and outcomes of hybrid warfare, i.e. the "ways and means to achieve an effect", which is intended to enhance an overall generalization of the concept and also simultaneously to increase its applicability (Johnson, 2018, p.157).

In this sense, hybrid warfare is now used to describe full-spectrum warfare, which encompasses a wide range of integrated military and non-military means of state power and clandestine actions available to a hybrid actor. The scope of tools and techniques available to hybrid warfare actors for the achievement of their respective objectives – political, economic, societal, informational – has, in turn, also significantly broadened with the evolution of information technologies and the rise of non-

state actors such as hacktivists, who challenge nation-states by strategically targeting vulnerabilities of governmental websites. A distinctive feature of cyber activities is that they can be carried out clandestinely and covertly. As a result, states can potentially lose a war before even knowing that it has already begun. Besides hacktivism, social media is another important instrument of hybrid warfare as it can equally be employed as a 'weapon'. This again reinforces a central idea behind the hybrid warfare as states use *weaponized* information to "deploy in a rapid-fire series of mutually-reinforcing stories that are hard for people to disregard and reach a global audience in seconds at minimal cost" (Herrmann, 2017).

But before going further into detail about the non-military means by which states and non-state actors conduct hybrid warfare, the relationship between hybrid and conventional warfare needs to be clarified. Conventional war can be conducted by using any conventional weapons excluding weapons of mass destruction (WMD) and is primarily waged against the adversary's military forces in an open confrontation. In contrast to the regular warfare, the hybrid warfare is a mix of both conventional and unconventional warfare that simultaneously combines the use of "conventional capabilities, irregular tactics and formations, and terrorist acts including indiscriminate violence, coercion, and criminal activity" (Hoffman, 2007, p.8). Accordingly, the use of force can be defined as 'hybrid' as long as warfare is not conducted one-dimensionally through purely military means or non-military tools that are available to a state or non-state hybrid actor. *Figure* 2 attempts to capture the kinds of actions a hybrid actor can undertake.

Accordingly, alongside with irregular and regular military forces, there is a variety of non-military tools that a hybrid actor can use in conflicts. Firstly, an actor can attempt to utilize financial and trade pressure as part of its hybrid tactics, for instance, by imposing economic sanctions on a target country or stopping a gas supply. Secondly, an actor can choose from a wide range of operations in the cyberspace by computer hacking or launching a cyber espionage campaign. Thirdly, an actor may strategically exploit cyber-enabled information warfare operations by weaponizing social media and news outlets, which use leads to social- and psychological manipulation of people. At this point, it is important to highlight that hybrid warfare combines several tools and, therefore, takes place across multiple 'battlefields' at the same time, which consequently makes it more complex and harder to respond to. Furthermore, it is important to keep in mind that the instruments of power that a hybrid actor may leverage against an opponent's vulnerabilities are highly context-dependent. Therefore, this paper seeks to analyse the elements of hybrid warfare separately as the term of hybrid warfare implies a variety of security threats such as grey zone operations and cyber-attacks. Accordingly, the main focus of the following chapter is placed on cyber attacks in order to assess the impact and func-

tional capabilities of a hybrid warfare actor.

Figure 2: Actions and tools available to a hybrid actor

Actions:	Tools:
Economic disruption	- Economic sanctions - Leveraging and using natural resources as a foreign policy tool
Strategic Weaponization of Information	Propaganda and disinformation campaigns: - Sponsoring news outlets : a) To spread of fake news b) To spread of conspiracy theories Social media manipulations: - Using of troll farms, advertisements, bots to spread polarizing messages
Cyber Operations	Cyber attacks/ cyber crime: - Hacks into critical infrastructure, political organizations, politicians - Cyber espionage: a) To gather intelligence b) To strategically leak private information c) To alter stored information
Social/Psychological Manipulation	- Supporting local upheavals - Gaining local support - Exploiting social cleavages, nationalist identities, and much debated topics over controversial policies
Irregular forces	Terrorists, Guerrilla Fighters, Insurgents, Unmarked soldiers
Regular military forces	Army, Navy, Air Force

Source: own construction based on a research

3. Cyber Warfare

Just as with hybrid warfare, there is no clear definition of cyber warfare either. The most cited and commonly accepted definition of cyber warfare comes from Clarke and Knake's book '*Cyber War: The*

Next Threat to National Security and What to Do About It'. Clarke and Knake (2010) define cyber warfare as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (p. 292). But this definition is quite limited, as it does not include non-state actors, e.g. hacktivists, groups and corporate espionage. Moreover, there is an open discussion whether cyber warfare itself can be seen as a 'real war' as there are no physical 'front lines' to it (Schneier, 2010; Missiroli, 2019). This paper argues, however, that the very notion of cyber warfare suits Carl von Clausewitz' definition of war, as "war is thus an act of force to compel our enemy to do our will" (Clausewitz et al., 1984) and that is exactly what cyber warfare does: compels an opponent to fulfil the attacker's will, as an attacker regards cyber attacks as an integral part of its offensive strategy to the achievement of its national objectives.

Additionally, alongside with three distinct battlefields of the hybrid warfare: the conventional battleground, the indigenous population caught in a conflict, and the international community (McCuen, 2008, p.107), cyberspace has recently been recognized as a new battlefield area for competition among states and has been officially declared as a "fifth operational domain", equal to land, sea, air, and space, which makes it to a space where a 'war' between states can take place. Ultimately, cyber warfare has transformed into an additional challenge to international and national security, and cyber attacks have added a new dimension to the overall concept of war as they seem to turn into one of the most preferred methods of warfare. The reasons for that are addressed in the next subchapter.

3.1 The Rise of Cyber Domain as a New Strategic Challenge

In comparison to conventional wars, cyber operations are relatively cheap to undertake, quite widely accessible to both states and non-state actors but, at the same time, they also generate higher impact and an opportunity to wage war covertly, i.e. without a physical confrontation and a declaration of war. Additionally, the actor behind cyber attacks is hard to identify, trace down and be proven guilty due to the usual absence of direct evidence and a straightforward international legal framework (Grisby, 2017; Georgieva, 2020). Thus, there is no clear set of rules of war and regulatory compliance mechanisms applicable to cyber warfare as the possibility and the extent to which the UN Charter or the Law of Armed Conflict or the Universal Declaration of Human Rights (UNDHR) can be effectively applied to cyber conflicts remains highly debated. Therefore, Geers (2015) argues that states will prefer to wage cyber wars as "they offer varying degrees of covertness and their treatment under international law remains ambiguous" (p. 41). Yet, an international consensus regarding

the legal status of cyber warfare is potentially forthcoming and is already in the process of discussions within numerous conferences on cyber security across the world.

The current absence of norms of 'good behaviour' and transparency, however, increases the uncertainty about the intentions of another state, which, in turn, drives states to a classical security dilemma (Buchanan, 2016). Hence, Leuprecht et. al. (2019) argue that the main challenge that cyber weapons and cyber operations possess is the uncertainty as of whether the actors use cyber space for offensive or defensive purposes (p.385). Moreover, there is uncertainty about the target country's or international community's response to cyber attacks. Can it be a war crime? Should or can NATO invoke Article 5? Will it rather create a boomerang effect? Can states file a retaliation complaint? Therefore technology-aided warfare can be characterised as a "double-edge sword'' as information dominance increases your hard and/or soft power, but at the same time, makes you vulnerable (Rattray, 2001; Dunn Cavelty and Wenger, 2020, p.15). Yet many states are developing their cyber capabilities due to the strategic benefits of cyber weapons. However, alongside the development of cyber programmes and rules of engagement regarding the use of cyber space, the cyber space and IT sector are rapidly changing and become more complex and increasingly sophisticated. That is why it is widely agreed that cyber-enabled technology is inevitably going to change the international and national security environment. In this context, the following chapter aims to present the types of cyber attacks and investigate the emerging trends in cyber warfare.

3.2 Types of Cyber Attacks and Trends in Cyber Warfare

Nowadays, cyber attacks are a matter of growing international concern due to their increasing sophistication and greater frequency. This, in turn, was a result of the evolution of attack technologies, the occurrence of state-sponsored cyber campaigns targeting government units, and greater interconnectivity among hackers, which have made cyber threats more "ubiquitous" and severe. Therefore, this chapter seeks to shed light on the shifting meaning of cyber security that has been changing along with an evolving set and frequency of cyber attacks. The challenge of cyber attacks to national cyber security used to be discussed primarily almost exclusively among American think tanks and war colleges in term of "what-if" scenario. However, the frequency of such events, like Russian attacks on web pages of Estonian official institutions in 2007, Stuxnet in 2010 – a malware aiming at nuclear facilities, large-scale DDoS attacks on JP Morgan and Bank of America in 2012 by Iranian hackers, several cyber attacks on Saudi Arabia's national oil company in 2012, and Snowden disclosures in 2013 have shifted the focus towards research that can be useful in the policy-making process.

Against this background, national governments have given increasing political attention to developing and strengthening national cyber capabilities for defensive and offensive purposes. As a result, numerous national cyber security centres, (e.g. Germany's Nationales Cyber-Abwehrzentrum in 2011, the U.S. Cyber Command in 2008 or the UK's National Cyber Security Centre in 2016), as well as bilateral initiatives (e.g. the U.S. - Japan Cyber Defense Policy Working Group in 2013 or the Warsaw Process Working Group on Cyber security in 2019) and international missions/organizations (e.g. NATO's Cooperative Cyber Defence Centre of Excellence in 2008 or the European Cyber Security Organisation in 2016), were established. Yet more and more states are trying to increase their cyber power as cyber warfare enables them to achieve their political objectives outside of the cyber domain because cyber warfare can significantly influence the distribution of power among states while not provoking a direct military confrontation (Dunn Cavelty and Wenger, 2020, p.12).

By all means, the actions of nation-state actors in the cyber domain have broadened the scope of cyber attacks. Firstly, there are non-state and state-sponsored actors performing strategic cyber attacks against critical infrastructure entities and hacking into corporate networks in order to steal information on specific individuals or plant viruses and spyware. Secondly, there are state-sponsored information warfare operations in the cyber domain, which are deliberately employed as data manipulation attacks, e.g. to intentionally influence public opinion by using trolls and bots to shape Internet content, and/or spreading misinformation in order to undermine public trust in national institutions. However, while the cyber space creates new opportunities for social manipulation, this paper defines cyber warfare in terms of the use of technology to attack and damage another nation's critical infrastructure and/or to access and expose personal information. This definition separates the blurred lines between cyber warfare operations and information warfare operations. Hence, cyber attacks/operations are defined as:

- "Examples of the use of new technologies within the scope of hybrid threats" (Döge, 2010 as cited in Bachmann and Gunneriusson, 2015, p. 82);
- "A modern form of political warfare, with major implications for coercive policy options and cyber strategies" (Atlantic Council Blog, 2018);
- Means to "manipulate, deny, disrupt, degrade, or destroy targeted computers, information systems or networks" (Hogeveen and Hanson, 2018);
- "Attempts to damage an adversary through attacking computers, information networks or any other facet of the modern Information Technology (IT) society" (Hughes and Shaffer, 2020, p. 300).

Accordingly, cyber weapons are used as tools of coercion and cover a wide range of activities that state- and non-state actors can utilize to inflict damage (Claver, 2018, p. 158; Leuprecht et. al, 2019, pp. 382-383). Cyber attacks can be divided into "syntactic attacks" via malicious software, which implies viruses and worms attacking users; and "semantic attacks" that attack infrastructures or IT facilities by modifying data unnoticeably, e.g. phishing and malvertising (Knopová and Knopová, 2014, pp. 25-26). Besides that, there is also an alarming trend of cyber espionage by state-sponsored cyber groups. *Table 1* provides a detailed overview of this trend based on the results of the research analysis presented by Osawa (2017). As of 2018, there were 41 cyber hackers associated with the Russian, Chinese, Iranian, and North Korean governments, who have allegedly conducted state-sponsored espionage just against the United States by targeting government agencies, banks, health care industry, international organizations and businesses in order to achieve their respective political objectives (Kiefer et. al., 2019).

Osawa (2017) argues that an overriding trend towards state-sponsored cyber attacks can be proven by the fact that these attacks "frequently follow incidents of international discord or conflict" (p. 115). Thus, the annexation of Crimea in 2014, in particular, became the focus of the renewed conflict between Russia and the US. Since then, Russia has been accused of large-scale cyber attacks against the U.S., as well as Ukraine and NATO member states. The most prominent of these accusations is Russia's attempts to access the critical infrastructure and elections systems in Ukraine. According to the report provided by the International Foundation of Electoral System, several days before the presidential elections in 2014 Russian hackers allegedly launched a cyber attack on Ukraine's Central Election Commission to influence the outcome of an election. More details on this trend will be provided in Chapter 4.

The growing importance of the "Dark Web" and an increasing amount of opportunities that it creates for people constitutes another emerging trend in cyber warfare. The "Dark Web" does not only contribute to cyber-attacks becoming more frequent, as it provides criminal groups and terrorists with a possibility to remain undetected and go unpunished but, moreover, it stimulates their professional development. As the "Dark Web" serves as a discussion forum and offers access to the latest hacking tools, cyber groups develop more sophisticated hacking methods and techniques and, as a result, become more organized and professionalized. Lastly, there is a trend of increased use of artificial intelligence (AI), which can serve as a cyber defence tool that helps to detect and resolve malware and/or cyber incidents. However, when it comes to AI, there are some questions as to whether hackers would use artificial intelligence to conduct large-scale cyber attacks. Therefore, the potential use of artificial intelligence broadens the scope for future cyber attacks and makes its use highly contro-

versial.

Table 1. Major State-sponsored Cyber Attacks (2007-2017)

(Year/Month)
- 2007.4 Estonia; cyber sabotage targeting government, media, financial sector.
- 2008.7 Lithuania; cyber sabotage targeting government, private sector.
- 2008 U.S. DoD; cyber intrusion and espionage.
- 2008.8 Georgia; cyber sabotage targeting government, media, financial sector.
- 2009.1 Kyrgyzstan; cyber sabotage targeting Internet Service Providers.
- 2009.7 ROK and U.S.; cyber sabotage targeting government.
- 2009.12 Google, cyber intrusion on its core system. Google retreated from business in China.
- 2010.8 Iran; Stuxnet, cyber subversion targeting Iranian uranium-enrichment plant.
- 2011.9 Japan; cyber espionage targeting defense industry, including MHI and IHI.
- 2011.10 Japan; cyber espionage targeting parliament member.
- 2011–12 U.S.; Iranian state-sponsored actor conducted cyber sabotage against financial sector.
- 2012.8 Saudi Arabia and Quarter; cyber subversion targeting energy industry, Saudi Aramco, RasGas.
- 2012.12–13.1 U.S.; cyber espionage targeting major newspapers and think tanks.
- 2013.3 ROK; cyber sabotage targeting media and financial sector.
- 2014.3 Ukraine; cyber sabotage targeting government and telecommunication company.
- 2014.5 Belgium; cyber espionage targeting Ministry of Foreign Affairs
  cf. 2010- European countries; cyber espionage targeting government, int'l organization.
- 2014.8 U.S.; cyber intrusion and financial cyber crimes targeting JP Morgan, etc.
- 2014.10 U.S.; cyber intrusion and espionage targeting White House and State Department.
- 2014.11 U.S.; cyber subversion targeting Sony Pictures Entertainment. U.S. government identified the attacking group and sanctioned North Korea (the first attributed state-sponsored attack).
- 2015.4 France; cyber subversion targeting TV5.
- 2015.4 U.S.; cyber intrusion and espionage targeting U.S. Office of Personnel Management, resulted in the theft of sensitive information of 21.5 million individuals.
- 2015 Germany; cyber espionage targeting Germany. Germany BND accused Russia.
- 2015.5 Japan; cyber espionage targeting Pension Service, 1.25 million records breached.
- 2015.12 Ukraine; cyber subversion targeting power grid company. (the first officially attributed state-sponsored attack on Critical Infrastructure)
- 2016.2 Bangladesh; cyber theft targeting the central bank, $81 million stolen.
- 2016.3 Sweden; cyber sabotage targeting media sector.
- 2016.4 Lithuania; cyber sabotage targeting its parliament.
- 2016.8 Viet Nam; cyber sabotage targeting international airports.
- 2016.11 Saudi Arabia; cyber subversion targeting government and private sector.
- 2016.11 U.S.; Russian cyber intrusion and espionage targeting Democratic National Committee.
- 2016.12 Ukraine; cyber subversion targeting power grid company in Kiev.
- 2017.4 Japan; new style cyber espionage operation named "Cloud Hopper" by APT10.
- 2017.5 World-wide; cyber subversion by the Wannacry ransomware cyber pandemic.
- 2017.6 World-wide; cyber subversion by the Petya/Not-Petya ransomeware cyber pandemic.

Source: Author, using open source materials.

4. Information Warfare Operations in the Cyber Domain

As mentioned above, information warfare operations using the cyber domain are a continuously emerging threat to the extent that it is often considered as a separate dimension of hybrid warfare. Information warfare aims to spread misleading information in a strategically chosen country in order to influence public opinion (Kostyuk and Zhukov, 2019, p. 319). In doing so, it seeks to influence people's perceptions, belief systems and emotions, i.e. it has an emotional and psychological impact on people's ability to build an opinion and reasoning (Svetoka et.al. 2016, p. 17). As a result, information becomes both a resource and a weapon, which can be employed as a powerful political and military tool, and thereby can indirectly undermine the opponent's domestic support for a particular course

of action (Lucas, 2017; Svetoka et.al., 2016).

It is widely argued that an intentional falsification of information, manipulation of media, and spread of disinformation can increase state's power projection capabilities by helping them to achieve their goals and objectives in a long-term perspective as these manipulations run for an unlimited amount of time (Hansen, 2017, p. 28). Cyber attacks, in contrast, achieve short-term changes but they make a more significant difference in the battlefield as, in comparison to information operations, cyber attacks can bring immediate substantial financial loss and damage to public reputation. Yet, we can also argue that social manipulation activities cause an effect close to military action as they simultaneously shape the target's behaviour and cognition, i.e. its perceptions of international and domestic politics (Mazarr et al., 2019). For instance, information operations activities in the propaganda category can cause political and societal division in a target country as they seek to influence public opinion and play on the vulnerabilities inherent to many states. Therefore, we can argue that both elements of hybrid warfare – cyber and information warfare – became an important aspect of war and can considerably reduce the necessity for deploying armed forces. But it is highly contextual as it is hybrid actor's choice whether to employ them individually or combine them.

Both conspiracy theories and fake news have been increasingly used in public opinion manipulations campaigns and are a form of information operations that encompass a cognitive part of hybrid warfare. The increased creation and consumption of fake news, in turn, is a direct consequence of the expansion of digital technology, which has created both new opportunities and challenges for policy makers, as the circumstances in which war can take place has evolved from kinetic to non-kinetic means (Holbrook, 2018). Furthermore, the technological development of information technology (i.e. the world population can, nowadays, be reached through the Internet and influenced in real-time) has also significantly changed the very concept of a classical war (Patrikarakos, 2017). Consequently, information platforms, such as social media and the Internet, which are employed in addition to more traditional weapons of war, became a commonly used tool of hybrid warfare (Singer and Brooking, 2018).

It is commonly known that Russia and China are engaged in social manipulation, which includes activities such as the distribution of conspiracy theories, conduction of targeted social media campaigns and data leaks. But whereas China is primarily controlling information domestically via its censorship system commonly known as the Great Firewall of China, Russia also attempts to manipulate information by interfering with other nation's affairs. A case that has gained high-profile publicity and largely contributed to the heated debates around Russia's assertive cyber and information warfare

capabilities is – an accusation of Russian interference in the US presidential elections in 2016 in order to help Donald Trump to win. However, unlike the above-mentioned types of cyber attacks, where actors gain access to a computer system to interfere or modify data, leaks exploit the same mean – hacking – but pursue a different goal. The following chapter aims to examine the Russian government's information warfare tactics in the cyber domain.

4.1 Cyber-Enabled Information Warfare Operations by the Russian government: A Case Study

Watts (2018) argues that, in contrast to Western countries, Russia is using cyber and information warfare more effectively because information and cyber technologies constitute an integral part of Russia's hybrid warfare rather than sub-constitutive one. Information warfare is commonly perceived as a broad and inclusive concept, which covers a range of hostile operations by using information whether as "a tool, or a target, or a domain of operations" (Giles, 2016, p. 6). However, the Russian government adopts a holistic approach to information warfare, which does not only "affect[s] the target state and its armed forces' ability to manage information and exercise effective command (…) but also to achieve[s] desired effects in the mind of target populations' perceptions and decision-making processes that favour Russia's interests and goals" (Tashev et al., 2019, p.139). Therefore, instead of conceptualizing cyber operations within the framework of cyber warfare, the Russian government includes them with the broader framework of information warfare that includes disinformation and psychological campaigns, cyber espionage, as well as cyber attacks on critical infrastructure facilities and election-related technology.

For instance, as Russia's hybrid warfare approach to Ukraine shows, Russia has designed a multifaceted cyber attack plan, which has involved a combination of activities such as disinformation, use of proxies and insurgencies along with military actions and economic manipulations. The Ukrainian conflict started with the military invasion of Crimean peninsula by Russian troops. However, alongside the Spetsnaz forces conducting seizures in Crimea and disrupting communication lines, hacktivists and cyber-criminals have been an important feature of Russian offensive cyber and military operations. As the conflict continued to escalate, both sides were engaging in low-intensity cyber attacks like distributed denial of service (DDoS), hacks of CCTV cameras and website defacements. Ukrainian cyber actions included specific attacks on communications and private companies by pro-Kyiv hackers like Anonymous Ukraine and Ukrainian Cyber Forces (UCFs), whereas pro-Russian cyber actors CyberBerkut, Green Dragon and Cyber Riot Novorossiya targeted Ukrainian media, government officials and private citizens (Kostyuk and Zhukov, 2019, p. 324). However, the cyber attacks on the

Ukrainian power grid in December 2015 and 2016, when state-sponsored hackers have remotely accessed and disrupted the control systems of Ukraine's grid operator, have shown how advanced and sophisticated Russian offensive cyber capabilities have become.

It is also worth mentioning that strategic information warfare, which was deployed as a foreign and domestic policy tool, constituted an equally important element of the Russian hybrid warfare. Perry (2015) argues that information manipulation tactics, which framed the narrative about the conflict, ensured the success of the Russian hybrid warfare operation in Ukraine, since they have created favorable pro-Russian sentiments among the targeted groups and considerably reduced the enemy's fighting potential. For instance, Russia was especially successful in conducting information operations within Ukraine by leveraging newspapers and TV stations to spread Russian propaganda, which has helped them to secure civic support for its military actions. But this international campaign, which involved the Internet trolling and Russia Today's TV reports promoting a deceptive narrative, was also waged against the international community and proved to be as effective as the military actions (Perry, 2015). It must, therefore, be concluded that the incorporation of cyber and information warfare into a hybrid warfare doctrine has not only blurred the line between wartime and peacetime but has also made the distinction between the concepts of cyber and information warfare extremely blurry. Therefore, the next subchapter takes a closer look at Russian information warfare and examines a variety of information tools that the Russian government uses as a part of its information warfare strategy.

4.2 Russian Information Warfare: Hacks and Leaks

As the details of the state's information warfare capabilities are mostly classified, newspapers offer a possibility to build possible links between the state's offensive and defensive use of information warfare tools. Therefore, news articles on information warfare published on Russia Today and Sputnik from December 2018 to April 2020, as well as articles written by Reuters, CNN, the Guardian and the Washington Post have been analysed. By analysing Russian newspapers, it can be concluded that Russian news are framed around stories that portray the United States and NATO member states as those who wage hybrid warfare against Russia, and information warfare is said to constitute a significant part of the West's efforts to encourage anti-Russian sentiments. The Russian government, in turn, claims that it does not wage any information attacks against the West; all it aims to achieve is an accurate representation of reality by providing factual, unbiased and more reliable information (Taran and Medvedeva, 2019). Therefore, by analysing news articles, the goal was to find common

patterns in terms of formulation of 1) goals, which both sides want to achieve 2) reasons behind the use of information warfare 3) tools that both sides are using.

According to the Russian news, the most commonly mentioned goals that the United States tries to achieve via its information attacks is to significantly weaken Russia's geopolitical position by imposing its viewpoint of global order (RT, 2019; Sputnik, 2019; Taran and Medvedeva, 2019; Orlov et al., 2019). At the same time, the other half of the articles insists that Western countries use information warfare as a political distraction from their many serious domestic problems (Sputnik, 2019). For instance, the U.S. discourse around Russia meddling in the 2016 presidential election and 2018 congressional elections was claimed by Russian media to have been aimed to unite the nation amid domestic problems and party competition by portraying Russia as an enemy of a nation. This is in accordance with articles by CNN that constantly appeal to defend "our nation, (…) our elections" due to the Russian misinformation campaigns that aim to "divide the party and nation". According to the FBI director, Christopher Wray, the success behind Russia's information warfare strategy lies in an ability of the Russian government to "identify issue that (…) American people feel passionately about on both sides and then they take both sides and spin them up so they pit us against each other," which, in turn, "weaken[s] our confidence in our elections and our democratic institutions" (The Guardian, 2020).

As of tools, there are three types of information warfare tools that are reported to be used by the Russian government: 1) leakages of personal information, 2) hacking attacks, i.e. creation of automated accounts and bots on social media platforms like Twitter, Facebook and YouTube, 3) spread of fake news and conspiracy theories via state-backed broadcasters. Confidential information being hacked and leaked is definitely on an upward trend, which started with the US diplomatic cables being released by WikiLeaks in 2010 and Edward Snowden leaking classified National Security Agency documents to journalists in 2013 and was supported by various individuals or groups of hacker such as, for instance, 'John Doe', who has anonymously leaked 11.5 million records from the Panamanian law firm, Massack Fonseca, to the German newspaper Süddeutsche Zeitung in 2015, which, in turn, resulted in tax evasion and money laundering investigations of 143 politicians and 12 national leaders with offshore wealth. On an even bigger scale, according to the New York Times, the Russian hacking and interference in the run-up to the US presidential elections in 2016 have "changed the direction of American history" (Goldenberg, 2018).

In 2016 a hacktivist named "Guccifer 2.0", who claimed to be an officer of Russia's military intelligence agency (GRU), took responsibility for hacking the network of the Democratic National Commit-

tee and posting the stolen emails and documents of the Democratic Party on the WikiLeaks website. Several months later an account of John Podesta, Clinton's campaign chairman, has been compromised. This resulted in email leaks, which were posted by WikiLeaks once again. The U.S. intelligence claims that by doing so the Russian government was aiming to assist Donald Trump with winning the presidential elections and to damage Hillary Clinton's candidacy. While the FBI investigations did not establish a conspiracy between the Trump campaign and the Russians, they found suspicious social media activity, i.e. the tweets propagating anti-Clinton sentiments, spreading conspiracy theories and encouraging support of the Black Lives Matter movement. Indeed, in November 2017, the US Senate Select Committee on Intelligence presented a list of more than 3500 Twitter bots that have been traced to a Russia-based Internet Research Agency (IRA): a 'troll factory'. Since then, the narrative of controlled bots and Russia meddling in social media by influencing public debates have been widely debated. The Russian government denies all allegation of managing or funding bot networks. Yet President Vladimir Putin has once mentioned, "patriotic" Russian citizens, who acted independently, might have operated these manipulations.

There is no definitive evidence yet that the Russian government sponsors troll factories to spread propaganda that helped Donald Trump get elected. Yet the possibility of Russia's interference in the domestic politics of other countries still produces public, political, and media discourses around Russian interference and sows discord. Since then, various news channels, newspapers, and politicians have released data on Russian interference in the following elections: 2016 US presidential elections and UK Brexit vote, 2017 UK general elections, 2017 French elections, 2018 Ukraine parliamentary elections, 2019 EU elections. Consequently, the "weaponization" of social media and intelligence-driven leaks continues to shape the discourse. More recently, new tactical leaks have caught the attraction of social media and newspaper outlets. Allegedly a Russian hacking group, known as 'Fancy Bear' or 'APT28', targeted a Ukrainian gas company *Burisma Holding* with a phishing campaign (Perlroth and Rosenberg, 2020). The main targets of these cyber attacks, however, are - the former Vice President/a contender for the 2020 US presidential election Joseph R. Biden and his son Hunter Biden, who were board members of the Burisma Holding. Due to the timing of this hacking campaign, American news media have been reporting about Russia trying to meddle into the U.S. election campaign once again. According to the news reports, these attacks are claimed to be targeting Joe Biden's campaign, as Joe Biden is the Democratic presidential candidate.

Yet, the Russian government claims that it "has not and does not interfere in the domestic politics of other countries" (TASS, 2017). Instead, it accuses NATO member states of waging anti-Russia campaigns in order to justify the existence of NATO in general, as well as to increase defence expending

across European allies. The Russian government claims that the aim of these NATO informational campaigns, in turn, is 1) to damage Russia's reputation among Russian speaking countries 2) to encourage domestic protests and political upheavals as they are mainly targeted towards the ordinary Russians. Therefore, several Russian news articles define these information campaigns as an "informational-psychological influence" (*informacionno-psixologicheskoe vozdeistvie*) directed against Russian citizens, and which is claimed to be achieved primarily by the U.S. and the UK through the sponsorship of the Russian "non-systemic opposition", as well as local and international Russophobic media in countries such as Poland, Georgia, Estonia, Latvia and Lithuania (Gureeva and Gorshenin, 2019; Pushkov, 2020). Notwithstanding these accusations, almost every article reports that Russia has never intended to confront Western powers. On the contrary, Russia is said to always favor dialogue and safeguard the rule of law in the international arena (Orlov et al., 2019). Yet, it is hard to deny the fact that the Russian government itself has been deploying a disinformation campaign by spreading propaganda and conspiracy theories via sponsored social media platforms and television networks. This will be further elaborated in the following subchapter.

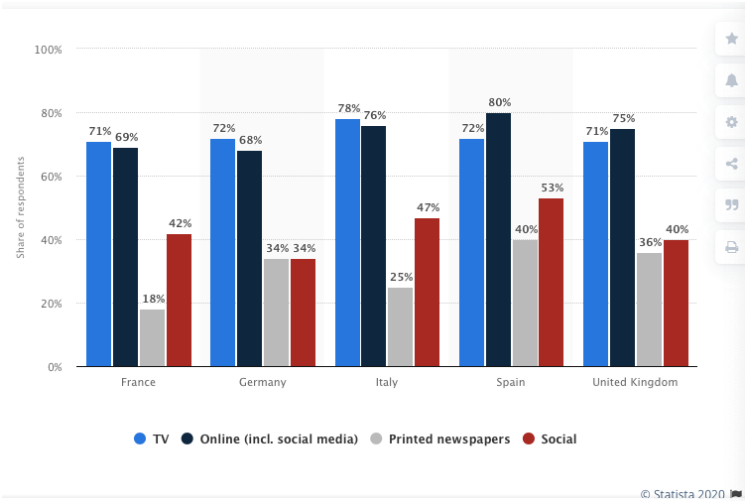
4.3 Russian Information Warfare: Conspiracy Theories and Propaganda

Spreading conspiracy theories and fake news is not a new phenomenon. Yet, modern computer technologies like social media and the Internet significantly increase destabilization and crisis-creating capabilities of information warfare, which could potentially help states to win the battle psychologically without even undertaking any military actions (Lanoszka, 2019, p. 241). According to Statista (2020), TV and Online sources (including social media) are the most popular news sources in the selected EU countries (i.e. Germany, the UK, Spain, Italy and France) and the penetration generally ranges between 68% and 80% (*Figure* 3). In response to these developments, social media platforms like Facebook and Google have introduced new fact-checking tools, and national governments began to revise social media laws and introduce a new set of rules on tighter regulation of social media platforms. However, rather than attempting to control Internet content, it is of greater importance to strengthen citizen's susceptibility to disinformation as notwithstanding the source of information, people tend to trust information that strengthens their own beliefs and reinforces their own identity. Therefore, we need to foster population's critical thinking skills both at the individual level and on a society-wide level in order to increase the reader's cognitive resilience skills as they are the targets of these cyber-enabled attacks alongside with all elements of country's national power (Hansen, 2017, p. 35).

The spread of conspiracy theories by the Russian government provides an example of more advanced information warfare attacks within the cyberspace. The Russian conspiracy theories become widespread mainly due to Russia Today (RT) - a state-funded news channel, which also broadcasts its pro-Russian narratives on YouTube. According to RT, the idea behind the channel is to provide audiences outside of Russia with a Russian point of view on major political events. RT perceives itself as a "truth-seeker", which uncovers disinformation campaigns spread by the Western countries. Yablokov (2015), on the other hand, argues that RT is a "propaganda machine" that the Russian government uses as a "specific tool of Russian public diplomacy, [which is] aimed at undermining the policies of the US government and, in turn, defending Russia's actions" (p. 301). Nevertheless, this channel has attracted wide public attention. For instance, its main channel has recently reached a 3 billion views benchmark. Furthermore, in addition to an English-language news channel, RT broadcasts in Russian, Arabic, French, German and Spanish, which, in turn, plays a crucial role in the promotion of the country's culture, positive image and geopolitical interests among foreign audiences. Thus, it is, for instance, argued that these pro-Russian/anti-EU news stories can potentially hinder a political integration of certain Western Balkan countries, i.e. Serbia, which is, however, reached via another Russian media platform – Sputnik Serbia (Zoric, 2017, p. 15).

Furthermore, conspiracy theories can serve as an effective approach to shape foreign audiences' behaviour, opinion and perception of international and domestic affairs. For instance, it is often claimed that Russia has allegedly waged an information war against Chancellor Merkel by inventing an "Our Lisa" campaign in a support of an underage Russian-German girl, who was falsely said to have been abducted and raped by Muslim refugees. Snyder (2018) argues that this disinformation campaign has weakened Angela Merkel's position towards migrant policy and, as a result, her support rate among citizens (i.e. Germans and the Russian-Germans), has significantly dropped. Numerous newspapers also attributed the rise of the Alternative for Germany (AfD) to the Russian manipulations of public opinion. It is claimed that Russian news outlets have been prominent in spreading "an alternative view of German reality, often depicting life under Chancellor Angela Merkel as dangerous, depraved and undemocratic while airing uncritical or laudatory reports about the AfD" (Shuster, 2017). Although there is little evidence about an actual correlation between Russian influence operations and rise of populist attitudes in Germany, we can argue that conspiracy theories can be used as an effective approach to the promotion of strategic narrative that seeks to reinforce country's global prestige and its views on international affairs.

Figure 3: News sources used in European countries in 2019



Source: Statista, 2020, [Online]
https://www.statista.com/statistics/422687/news-sources-in-european-countries/

5. Conclusion

The concept of hybrid warfare has been exposed to criticism in regard to the lack of conceptual clarity. While the definition of hybrid warfare needs to be revised indeed, hybrid warfare as a concept creates valuable insights into tools of foreign policy available to a hybrid actor, and highlights current and emerging security challenges, as it uses an "analytical language that allows for flexibility in approaching how to think about and operate in the future security environment" (Reichborn-Kjennerud and Cullen, 2016, p.4). By analysing the literature on hybrid warfare and studying the case of Russia, this paper undertook an effort to bring greater conceptual clarity to the concept of hybrid warfare.

Undoubtedly, the economic, social and military domains constitute important tools of hybrid warfare. The domains of cyber of information warfare, however, are considered to be two of the most central tools that have contributed to the evolution of the hybrid warfare concept. Hence, while this paper has focused on hybrid warfare, it put a special emphasis on aspects of cyber and information warfare. The conducted research on cyber and information warfare, in turn, has brought to light the haziness between these two concepts. Cyber warfare is often referred to as cyber espionage in terms of computer-based cyber-attack against critical infrastructure in order to access and expose personal information. Yet, nowadays, nation-state actors do not only sponsor hacking groups to target adversary's computer networks and systems but are increasingly engaged in cyber-enabled information

warfare by sponsoring political ads, bot accounts, and troll factories on social media platforms like Twitter and Facebook to spread disinformation and propaganda. Consequently, the targets of these hybrid attacks are both civilian population and all elements of adversary's national power.

Accordingly, while analysing these specific features of hybrid warfare, the paper simultaneously illustrated the growing significance and on-going trends in cyber and information warfare. In doing so, it highlighted the fact that social media has become one of the most important instruments of hybrid warfare due to its power to construct public beliefs and understanding, as well as to shape public perceptions and attitudes towards political and social issues. On the other hand, the cyber domain can also be successfully used to convey domestically defined foreign and security objectives to foreign audiences (Popescu and Secrieru, 2018, p.6). To illustrate that, the case of Russia was chosen and analysed, as it provides the best example of a comprehensive hybrid warfare strategy and gives more explicit details of the use of cyber and information warfare as part of hybrid warfare strategies.

The findings of this paper implicate that the Russian government employs a broad range of non-military instruments to pursue its national interest, many of which belong to cyber and information warfare. But it is worth mentioning that while all states seek to enhance their cyber and information capabilities, Russia possesses a "qualitatively new phenomenon" as it simultaneously incorporates both domains into its hybrid warfare strategy (McNair, 2017). Indeed, among the non-military tools and techniques that Russia frequently uses as a part of its hybrid activities are: hacking email accounts, spreading fake news through social media in proximity to important elections by using trolls and bots, leaking potentially damaging information, dissemination of misleading information and conspiracy theories via state-sponsored television and news channels like RT and Sputnik. Therefore, we must pay closer attention to the hybrid warfare strategies of the Russian government due to their strategic uniqueness and unpredictability.

Figure 1: Definitions of Hybrid warfare

Author/ Year	Definition of Hybrid Warfare
Nemeth (2002, p. 29)	Hybrid Warfare is - "the contemporary form of guerrilla warfare, is a continuation of pre-state warfare that has become more effective because it employs both modern technology and modern mobilization methods".
UK Ministry of Defense (2007)	Hybrid warfare is "conducted by irregular forces that have access to the more sophisticated weapons and systems normally fielded by regular forces. Hybrid warfare may morph and adapt throughout an individual campaign, as circumstances and resources allow. It is anticipated that irregular groups will continue to acquire sophisticated weapons and technologies and that intervention forces will need to confront a variety of threats that have in the past been associated primarily with the regular Armed Forces of states" .
Hoffman (2009, p.35)	Hybrid warfare is a construct "in which the adversary will most likely present unique combinational or hybrid threats [...] instead of separate challenges with fundamentally different approaches (conventional, irregular, or terrorist), we can expect to face competitors who will employ all forms of war and tactics, perhaps simultaneously".
NATO (2010).	Hybrid threats are "those posed by adversaries with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives" Hybrid threats are "those posed by adversaries with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives".
Mansoor (2012, p.3)	Hybrid warfare is "a conflict involving a combination of conventional military forces and irregulars (guerrillas, insurgents, and terrorists), which could include both state and nonstate actors, aimed at achieving a common political purpose. [It] plays out at all levels of war, from the tactical, to the operational, to the strategic".
McCulloh, T. B. and Johnson, R. B. (2013, p.17)	Hybrid warfare is "a form of warfare in which one of the combatants bases its optimized force structure on the combination of all available resources—both conventional and unconventional—in a unique culture context to produce specific, synergistic effects against a conventionally-based opponent".
IISS (2015, p.5)	Hybrid warfare is "the use of military and non-military tools in an integrated campaign designed to achieve surprise, seize the initiative and gain psychological as well as physical advantages utilising diplomatic means; sophisticated and rapid information, electronic and cyber operations; covert and occasionally overt military and intelligence action; and economic pressure".
Rusi (2015, p. 13)	Hybrid warfare can be defined as a "'multilayered espionage' including intelligence and political-active operations combined with traditional and modern more technically executed espionage".
Morris (2015, p. 2).	Hybrid warfare is a type of warfare, which "employ[s] 21st

	century technologies and combinations of diplomatic, intelligence, militaristic, economic, informational, cyber and humanitarian means in all domains to create war on all fronts".
Abbott (2016, p. 3)	Hybrid warfare is a "form of warfare that includes a range of multi-modal activities that can be conducted by state or non-state actors. Emphasis is placed on simultaneous and unprecedented fusion of a variety of means such as political, military, economic/financial, social and informational using conventional, irregular, catastrophic, terrorist and disruptive/criminal methods to achieve political objectives. The hybrid actor fuses these means and methods in a way that is specific to and tailored-made to the context at hand".
Lanoszka (2016, p.178).	Hybrid warfare is "a strategy rather than a new form of war. It is a strategy because it deliberately integrates the use of various instruments of national power so as to achieve foreign policy objectives in the light of the believed goals and capabilities of the adversary. It can cover a range of expedients so long as they are guided by an overarching goal".
Vuković et al. (2016, p. 119)	Hybrid warfare is "a form of conflict in which regular and irregular military forces are involved together in order to achieve the same strategic objective".
Angstrom (2017, p.844).	Hybrid warfare is "a form of communication in which the parties gradually develop a new, common language and learn to speak in it, thus opening the path to reaching a political settlement. It is a new language that both parties learn from one another and create (or construct) in their interaction".
Aoi et al. (2018, p.706)	Hybrid warfare is "the blending of conventional and non-conventional methods to achieve political-military objectives by both state and non-state actors; as such, it implies an ends-means link inherent in a strategy ".
Magda (2018, p. 63)	Hybrid war is a "set of state actions of the military, information, diplomatic, economic character aimed to solve the tasks of the submission one state's interests to another, which does not exclude the formal preservation of the sovereignty of the victim of aggression".
Kols (2018)	Hybrid warfare can be defined as "asymmetric and nontraditional military capabilities, [such as] information operations, cyber attacks, disinformation, propaganda, and psychological operations".
Johnson (2018, p.157)	Hybrid warfare "reflects new opportunities at both the strategic and operational level due to the combined effects of globalization, mass communications in the hands of more of the world's population, and the technological innovations of the internet, mobile telephony and cable and satellite television".
Goncharenko (2020).	Hybrid warfare is a "confusing cocktail of unmarked troops, local proxies, and blanket disinformation".

Source: own construction based on a research

Bibliography

Abbot, K. (2016) "Understanding and Countering Hybrid Warfare: Next Steps for the North Atlantic Treaty Organization", University of Ottawa, 23 March, [Online] http://www.natolibguides.info/hybridwarfare/articles/archives [Accessed: 14 April 2020].

Angstrom, J. (2017) "Escalation, Emulation, and the Failure of Hybrid Warfare in Afghanistan", *Studies in Conflict & Terrorism*, (40:10), pp. 838–856.

Aoi C., Futamura M. and Patalano A. (2018) "Introduction 'Hybrid Warfare in Asia: Its Meaning and Shape", *The Pacific Review* (31:6), pp. 693-713.

Atlantic Council Blog (2018) "The Challenges of Cyber Strategy", 22 August, [Online] https://www.atlanticcouncil.org/event/the-challenge-of-cyber-strategy/ [Accessed: 05 May 2020].

Bachman, S. D. and Gunneriusson, H. (2015) "Hybrid Wars: The 21st- Century's New Threats to Global Peace and Security, *Militaria African Journal Military Studies* (43:1), pp. 77-98.

Buchanan, B. (2016). *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (Oxford: Oxford University Press).

Clarke, R. A. and Knake, R. K. (2010) *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins).

Claver, A. (2018) "Governance of Cyber Warfare in the Netherlands: An Exploratory Investigation", *The International Journal of Intelligence, Security and Public Affairs* (20), pp. 155–180.

Clausewitz, C. v., Howard, M., Paret, P., and Brodie, B. (1984) *On War (*Princeton, N. J.: Princeton University Press).

Dunn Cavelty M. and Wenger A. (2020) "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science", *Contemporary Security Policy* (41:1), pp. 5-32.

Geers, K. (2015) *Cyber War in Perspective: Russian Aggression Against Ukraine*. In: Lewis, A. J. (ed.), 'Compelling Opponents to Our Will': The Role of Cyber Warfare in Ukraine (Talinn: NATO Cooperative Cyber Defence Centre of Excellence), pp. 39-47

Georgieva I. (2020) "The Unexpected Norm-settlers: Intelligence Agencies in Cyber Space", *Contemporary Security Policy* (41), pp. 33-54.

Giles, K. (2016) "Handbook of Russian Information Warfare", NATO Defense College (9), pp. 1-78.

Grisby, A. (2017) "The End of Cyber Norm", *Survival* (59), pp. 109–122.

Goldenberg, M. (2018) "Yes, Russian Trolls Helped Elect Trump. Social Media Lies Have Real-World Consequences", *The New York Times*, 17 December, [Online] https://www.nytimes.com/2018/12/17/opinion/russia-2016-election-influence-trump.html [Accessed: 05 May 2020].

Goncharenko, O. (2020) "The Lesson of Crimea: Appeasement Never Works", *Atlantic Council,* 27 February, [Online] https://www.atlanticcouncil.org/blogs/ukrainealert/the-lesson-of-crimea-appeasement-never-works/ [Accessed: 14 April 2020].

Gureeva, Y., and Gorshenin, K. (2019) ""Obiasnenie neudach": v Gruzii obvinili "rossijskuju propagan-

dy" v popytke pomezhat evrointegracii, *Russia Today*, 6 August, [Online] https://russian.rt.com/world/article/656287-gruziya-evrointegraciya-informacionnaya-voina-rossiya [Accessed: 05 May 2020].

Hansen, F. S. (2017) "Russian Hybrid Warfare: A Study of Disinformation", *Danish Institute for International Studies*, pp. 28-31.

Herrmann, J. (2017) "The Weaponized Narrative, Sun Tzu, and the Essence of War", *Real Clear Defense*, 27 July, [Online] https://www.realcleardefense.com/articles/2017/07/27/nine_links_in_the_chain_111911.html [Accessed: 05 May 2020].

Hoffman, F. (2007) *Conflict in the 21st Century: The Rise of Hybrid War*. Arlington: Potomac Institute for Policy Studies.

Hoffman, F. (2009) "Hybrid warfare and Challenges", *JFQ* (52:1), pp. 34-48.

Hogeveen, B. and Hanson, F., and Uren, T. (2018) "Defining Offensive Cyber Capabilities, *Australian Strategic Policy Institute*, 04 July, [Online] https://www.aspi.org.au/report/defining-offensive-cyber-capabilities/ [Accessed: 05 May 2020].

Holbrook, D. J. (2018) Information-Age Warfare and Defence of The Cognitive Domain, Australian Strategic Policy Institute, 13 December, [Online] https://www.aspistrategist.org.au/information-age-warfare-and-defence-of-the-cognitive-domain/ [Accessed: 25 May 2020].

Hughes G. and Shaffer R. (2020) "Cyber War and Lessons From History in the Digital Age", *Intelligence and National Security* (35:2), pp. 300–305.

IISS (2015) *Military Balance 2015* (London: International Institute for Strategic Studies).

Johnson, R. (2018) "Hybrid war and its countermeasures: a critique of the literature", *Small Wars & Insurgencies* (29:1), pp. 141-163.

Kiefer, K., Abbas, N., and Poole, E. (2019) "Cyber Alert: Ten Lessons from Six 2018 DOJ Indictments of State-Sponsored Hackers", *Alston & Bird*, 29 January, [Online] https://www.alston.com/en/insights/publications/2019/01/ten-lessons-from-six/ [Accessed: 05 May 2020].

Kostyuk, N. and Zhukov, Y. M. (2019) "Invisible Digital Front: Can Cyber Attacks Shape Batterfield Events?" *Journal of Conflict Resolution* (63:2), pp. 317-347.

Knopová, M. and Knopová *E*. (2014) "The Third War In The Cyberspace? Cyber Warfare in the Middle East", *Acta Informatica Pragensia* (3:1), pp. 23–32.

Kols, R. (2018) "NATO Must Meet Russia's Hybrid Warfare Challenge", *Atlantic Council Blog*, 3 July, [Online] https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-must-meet-russia-s-hybrid-warfare-challenge/ [Accessed: 14 April 2020].

Lanoszka, A. (2016), Russian hybrid warfare and extended deterrence in eastern Europe. International Affairs (92), pp.175-195.

Lanoszka, A. (2019) "Disinformation in International Politics", *European Journal of International Security* (4), pp. 227 - 248.

Leuprecht, C., Szeman, J., and Skillicorn, D. B. (2019) "The Damoclean Sword of Offensive Cyber: Poli-

cy Uncertainty and Collective Insecurity", *Contemporary Security Policy* (40:3), pp. 382-407.

Lucas, K. (2017) *The Virtual Weapon and International Order* (London: Yale University Press).

Magda, Y. (2018) The Roots of Confrontation: Energy Aspect of Hybrid Warfare", *Historia i Polityka* (26:33), pp. 63–71.

Mansoor, P. R. (2012) "Introduction: Hybrid Warfare in History", in Murray, W. and Mansoor, P. (Eds.) *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present* (Cambridge: Cambridge University Press), pp. 1-17.

Mazzar, M. J., Casey, A., Demus, A., Harold, S. W., Matthews, L. J., Mustafaga, N. B. and Sladden, J. (2019) "Hostile Social Manipulation. Present Realities and Emerging Trends", *RAND Corporation*, pp.1-302.

McCuen, John J. "Hybrid Wars." Military Review. Mar/Apr 2008, Vol. 88 Issue 2, 107-113.

McCulloh T. and Richard J. (2013) "Joint Special Operations University 7701 Tampa Point Boulevard MacDill AFB FL 33621", JSOU Report (13:4), pp. 1-137.

McNair, B. (2017) *Fake News: Falsehood, Fabrication and Fantasy in Journalism* (New York: Routledge).

Ministry of Defense (2007) The United Kingdom Joint Doctrinal Note 2/07 *Countering Irregular Activity Within A Comprehensive Approach*, Defence Academy (Shrivenham, Wiltshire, UK).

Missiroli, A. (2019) "From Hybrid Warfare to 'Cybrid' Campaigns: The New Normal?" *NATO Defense College Policy Brief*, pp. 1-4.

Morris, V. R. (2015) "Leveraging Lietuva: Establishing a 21st Century Nonlinear Warfare Centre of Excellence", *Small Wars Journal,* [Online] https://smallwarsjournal.com/jrnl/art/leveraging-lietuva-establishing-a-21st-century-nonlinear-warfare-centre-of-excellence [Accessed: 14 April 2020].

Nemeth, W. J. (2002) "Future War and Chechnya: A Case For Hybrid Warfare", unpublished thesis, Naval Postgraduate School, [Online] https://core.ac.uk/download/pdf/36699567.pdf [Accessed: 05 May 2020].

North Atlantic Treaty Organization (2010) "Bi-Sc Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats", [Online]http://www.act.nato.int/images/stories/events/2010/20100826_b i-sc_cht.pdf [Accessed: 05 May 2020].

Orlov, S., Gureeva, Y., Shurpina, A. (2019) ""Na urovne mainstreama": v Shveizarii prizvali Zapad perejti k politike "novogo sderzhivanja" RF", *Russia Today*, 9 February, [Online] https://russian.rt.com/world/article/652645-nato-gibridnaya-voyna-rossiya-5-prichin [Accessed: 05 May 2020].

Osawa, J. (2017) "The Escalation of State Sponsored Cyberattack and Cyber Security Affairs: Is Strategic Cyber Deterrence The Key to Solving The Problem?" *Asia-Pacific Review* (24), pp. 113–131

Patrikarakos D. (2017) *War in 140 characters: How Social Media is Re-shaping Conflict in the Twenty-First Century* (Basic Books: New York).

Perlroth, N., and Rosenberg, M. (2020) "Russians Hacked Ukrainian Gas Company at Center of Im-

peachment", *The New York Times*, [Online] https://www.nytimes.com/2020/01/13/us/politics/russian-hackers-burisma-ukraine.html [Accessed: 05 May 2020].

Perry, B. (2015) "Non-Linear Warfare in Ukraine: The Critical Role of Information Operations And Special Operations", *Small War Journal*, 14 August, [Online] https://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera#_edn81 [Accessed: 24 May 2020].

Popescu, N. and Secrieru, S. (2018) "Hacks, Leaks and Distributions. Russian Cyber Strategies", *Chaillot Papers* (148), [Online] https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf [Accessed: 05 May 2020].

Pushkov, A. (2020) *Missija Rossija. Xvatit li sil u Putina?* (Litres: Moscow).

Rattray, G. (2001) *Strategic Warfare in Cyberspace* (Cambridge, MA: The MIT Press).

Reichnorn-Kjennerud, E. and Cullen, P. (2016) "What is Hybrid Warfare?" *Norwegian Institute of International Affairs* (1), pp. 1-4.

Rusi, A. (2014) *Espionage as a Method of a Modern Hybrid War*. In: Wilfried Martens Centre for European Studies and Toivo Think Thank (Ed.)*, Seminar Paper,* pp. 11-14.

Russia Today (2019) "V MID ocenili soobzhenija ob informacionnoj taktike CSHA protiv Rossii", *Russia Today*, 26 December, [Online] https://russian.rt.com/world/news/702304-zaharova-rossiya-ssha-taktika [Accessed: 05 May 2020].

Schneier B. (2010) *Threat of 'Cyberwar' Has Been Hugely Hyped*, 10 July , [Online] http://edition.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/index.html [Accessed: 05 May 2020].

Shuster, S. (2017) How Russian Voters Fueled the Rise of Germany's Far-Right, *The Times*, 25 September, [Online] https://time.com/4955503/germany-elections-2017-far-right-russia-angela-merkel/ [Accessed: 05 May 2020].

Singer, P.W. and Brooking, E. (2018) *Like War: The Weaponisation of Social Media* (Mifflin Harcourt, Boston-New York).

Snyder, T. (2018) *The Road to Unfreedom: Russia, Europe, America* (New York: Tim Duggan Books.).

Sputnik (2019) "Russian Military Aware of Preparations for Info Warfare Against Top Brass- MoD", *Sputnik*, 26 June, [Online] https://sputniknews.com/military/201906261076058462-mod-aware-of-preparations-for-informational-attacks-against-russian-military-leadership---spokesman/ [Accessed: 05 May 2020].

Statista (2020) [Online] https://www.statista.com/statistics/422687/news-sources-in-european-countries/

Svetoka, S., Reynolds A. and Curika L. (2016) "Social Media as a Tool of Hybrid Warfare", *NATO STRATCOM Centre of Excellence*, [Online] https://www.stratcomcoe.org/social-media-tool-hybrid-warfare [Accessed: 14 April 2020].

Taran, I., and Medvedeva (2019) "Personalnaja diskriminacija: Minooborony RF zajavilo o gotovjashixsja informacionnyx atakax na voennoe rukovodstvo strany", *Russia Today*, 28 December, [Online] https://russian.rt.com/russia/article/702892-informacionnoe-davlenie-minoborony-rossii

[Accessed: 05 May 2020].

Tashev, B., Purcell, M. and McLaughlin, B. (2019) "Russia's Information Warfare. Exploring the Cognitive Dimension", *Marine Corps University Journal* (10:2), pp. 129-147.

TASS (2017) "Putin Stresses Russia Never Interferes in Other Counties' Domestic Policy", 28 February, *Russian News Agency*, [Online] https://tass.com/politics/933239 [Accessed: 05 May 2020].

The Guardian (2020) "Russian Engaging in 'Information Warfare' Ahead of 2020 Election, FBI chief warns", The Guardian, 14 January, [Online] https://www.theguardian.com/us-news/2020/jan/14/russian-hackers-targeted-ukrainian-company-burisma-impeachment-hunter-biden [Accessed: 05 May 2020].

Vuković J., Matika D. and Barić S. (2016) "Hybrid Warfare Challenges", *Security and Defence Quarterly* (12:3), pp. 118–138.

Watts, C. (2018) *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News* (HarperCollins: New York).

Yablokov, I. (2015) "Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of Russia Today (RT)", Politics (35:3-4), pp. 301-315.

Zoric, B. (2017) "Assessing Russian impact on the Western Balkan countries' EU accession: cases of Croatia and Serbia", *Journal of Liberty and International Affairs*, (3:2), pp. 9-18.