
JIPSS

JOURNAL FOR INTELLIGENCE,
PROPAGANDA AND SECURITY STUDIES

VOLUME 12, NUMBER 2 / 2018



Published by the
Austrian Center for Intelligence,
Propaganda and Security Studies

MEDIENINHABER, HERAUSGEBER UND VERLEGER

Austrian Center for Intelligence, Propaganda
and Security Studies (ACIPSS)

HERAUSGEBERKOMITEE DIESER AUSGABE

Paul Schliefstainer (Koordination)
Dieter Bacher
Wolfgang Göderle

VERLAGSANSCHRIFT

Institut für Geschichte
Karl-Franzens-Universität Graz
Attemsgasse 8/III, A-8010 Graz
office@acipss.org

BLATTLINIE

Das Journal für Intelligence, Propaganda and Security Studies (JIPSS) dient der Publikation von Forschungsergebnissen und der Diskussion von Fragen der Nachrichtendienste, Propaganda und Sicherheitspolitik.

EDITORIAL OFFICE

ACIPSS
Institute of History, University of Graz
Attemsgasse 8/III, A-8010 Graz, Austria
Telefon +43/ 316/ 380-8099
Fax +43/ 316/ 380-9730
office@acipss.org
www.acipss.org

LAYOUT

Alexander J. Pfleger
Melissa Pfleger

COVER

Standbild aus *Der dritte Mann* (© London Film Studios/
Studiocanal), künstlerisch interpretiert und adaptiert von
Alexander J. Pfleger

HERSTELLER

ÖH-Servicebetriebe Graz

ISSN 1994 4101

© ACIPSS

JIPSS EDITORIAL ADVISORY BOARD

Günter Bischof, University of New Orleans
Hans Fredrik Dahl, University of Oslo
Daniele Ganser, University of St. Gallen
Constantin Goschler, University of Bochum
Michael Herman, Nuffield College, Oxford University
Loch K. Johnson, University of Georgia
Wolfgang Krieger, University of Marburg/Lahn
Igor Lukes, Boston University
Timothy Naftali, New York University
John M. Nomikos, RIEAS, Athens
Miroslav Tadjman, University of Zagreb
Jerca Vodusek-Starič, University of Ljubljana
Michael Wala, University of Bochum
Cees Wiebes, NCTb, The Hague
Joseph Wippl, Boston University

REDAKTION/EDITORIAL COMMITTEE

Martin Moll (Chefredakteur/Executive Editor)
Johanna Fürst (Rezensionsredakteurin/Reviews Editor)
Jamie Harrison (Korrektur und Redaktion englischer
Beiträge/English Language Editor)
Dieter Bacher, Paul Schliefstainer, Jeremy Stöhs, Sarah
Strasser, David Jaklin, Carolin Schliefstainer (Redakteure/
Editors)

Die Beiträge geben die Meinungen der Verfasserinnen und Verfasser, aber nicht zwingend jene der Redaktion, von ACIPSS oder des Herausgeberkomitees wieder. Trotz intensiver Bemühungen und sorgfältiger Bearbeitung erfolgen alle Angaben und Informationen ohne Gewähr. Haftungen von ACIPSS, des Herausgeberkomitees, der Redaktion oder der Autorinnen und Autoren sind ausdrücklich ausgeschlossen. Die verwendeten Fotos, Bilder, Grafiken und Zeichnungen etc. wurden – außer in jenen Fällen, in denen es anders vermerkt ist – von den Autorinnen und Autoren geliefert, die laut Autorenrichtlinien ausdrücklich für die Beachtung und gegebenenfalls den Erwerb der notwendigen Bild- bzw. Reproduktionsrechte verantwortlich zeichnen. Bei allfälligen Verstößen gegen die Urheber- oder Werknutzungsrechte haben sich deren Inhaber direkt an die Autoren zu wenden.

All opinions expressed are those of the individual authors, and not necessarily those of the editors, ACIPSS's, or the editorial committee. Despite intensive efforts and careful processing, no responsibility is taken for the correctness of this data or information. Any liability of ACIPSS, the editorial committee, the editors or the authors is excluded. All photographs, images, graphics and drawings etc. used (except in cases where otherwise noted) are supplied by the authors, who are, as it is explicitly stated in the guidelines for authors, ultimately responsible for adhering to copyright laws and, if necessary, the acquisition of reproduction rights. In the event of any copyright or reproduction right infringements, the owners of said rights have to contact the individual author(s) directly.

INHALT/CONTENTS

- 6 EDITORIAL: PAUL SCHLIEFSTEINER**, *Der dritte Mann*: Ein Schwerpunktthema zum Filmklassiker
The Third Man: A Film Classic in Focus
-

Schwerpunkt/In Focus

- 9 THOMAS RIEGLER**, Die Spionagegeschichte hinter *Der dritte Mann*
- 29 LYDIA NOVAK**, *Der dritte Mann*: Das Regeldrama des Film Noir Autrichien
The Third Man: The Norm Drama of Film Noir Autrichien
- 42 EVA HORN**, Graham Greene's Heart of Darkness: Post-War Vienna in *The Third Man*
- 53 SIEGFRIED BEER**, The Heart of Friendship. Conjecture and Coincidence in *The Third Man*. A follow-up Essay
- 59 SIEGFRIED BEER**, "Given a Chance, She Should Make a Job of It". A British Diplomat's Assessment of Austria's Prospect for Survival in 1950
- 65 BRIGITTE TIMMERMANN**, *Der dritte Mann*: Die Frauen im Film, die Frauen hinter dem Film
- 76 CORDULA SIMON**, Klischee, Propaganda und Differenzierung in Graham Greenes *Der dritte Mann*
Cliché, Propaganda and Differentiation in Graham Greene's *The Third Man*
- 81 DIETER BACHER**, *The Prague Coup* – Ein Blick in das Wien der Nachkriegszeit und des frühen Kalten Krieges
The Prague Coup – A look at Vienna during the post-war years and the early Cold War
- 91 DAVID CHRISTOPHER JAKLIN**, *Der dritte Mann* – Auf den Spuren eines Filmklassikers
The Third Man – In the footsteps of a film classic
- 94 JAMIE HARRISON, STEFANIE HOFBAUER**, 3. Mann Tour: Auf den Spuren von Harry Lime
The Third Man Tour: In the footsteps of Harry Lime
- 99 MARIO MUIGG**, Das dritte Mann Museum in Wien
Third Man Museum, Vienna
-

Topical Essays

- 104 ULF WALTHER**, Auf dem Weg nach EU-Europa? Politische Einflussnahme und Islamismus auf dem Westbalkan
- 136 EBI SPAHIU**, Islamist Radicalization and Violent Extremism in Western Balkan Diaspora in Europe: Connections, Networks and Potential Security Concerns
- 145 SEBASTIAN VON MÜNCHOW**, Peter Ernst von Mansfeld 2.0: Zur Zersetzungskraft zeitgenössischer unterstaatlicher Akteure
- 155 SVEN BERNHARD GAREIS**, Hybrid Threats and Warfare. How States and Societies Can Cope with Conventional and Unconventional Security Challenges
-

Documentation

- 165 DAVID CHRISTOPHER JAKLIN**, 28. ACIPSS-Arbeitstagung am 8. Februar 2019 am FH Campus Wien
28th ACIPSS Workshop on February 8, 2019 at the FH Campus Vienna
-

Book Reviews

- 174** Christopher Andrew, *The Secret World. A History of Intelligence* (Siegfried Beer)
- 177** Michael Epkenhans, Gerhard P. Groß, Markus Pöhlmann, Christian Stachelbeck (eds.), *Geheimdienst und Propaganda im Ersten Weltkrieg. Die Aufzeichnungen von Oberst Walter Nicolai 1914 bis 1918* (Martin Moll)
- 179** Katrin Paehler, *The Third Reich's Intelligence Services. The Career of Walter Schellenberg* (Martin Moll)
- 182** Alexandra Bleyer, *Propaganda als Machtinstrument. Fakten, Fakes und Strategien. Eine Gebrauchsanleitung* (Madeleine Manowarda)
- 184** Seymour M. Hersh, *Reporter: A Memoir* (Loch K. Johnson)
- 189** Marc Stegherr, *Der neue Kalte Krieg in den Medien. Die Medien Osteuropas und der neue Ost-West-Konflikt* (Heinz P. Wassermann)
- 192** Sam Mullins, *Jihadist Infiltration of Migrant Flows to Europe – Perpetrators, Modus Operandi and Policy Implications* (Paul Schliefssteiner)

Sven Bernhard Gareis

HYBRID THREATS AND WARFARE. HOW STATES AND SOCIETIES CAN COPE WITH CONVENTIONAL AND UNCONVENTIONAL SECURITY CHALLENGES



Prof. Dr. Sven Bernhard Gareis

is a Professor of International Politics at the Westfälische Wilhelms-Universität in Münster, Germany. Being an expert on China and East Asia, he also works on international organizations' role in the maintenance of peace and security. Contact: svengareis@web.de

Zusammenfassung:

HYBRIDE BEDROHUNGEN UND KRIEGSFÜHRUNG. WIE STAATEN UND GESELLSCHAFTEN KONVENTIONELLEN UND UNKONVENTIONELLEN SICHERHEITSGEFÄHRDUNGEN BEGEGNEN KÖNNEN

Hybride Bedrohungen und Kriegsführung sind keineswegs neue Phänomene. In der globalisierten Welt mit ihren immer engeren Verkehrs- und Kommunikationsverbindungen indes sind ihre Auswirkungen immer schneller und unmittelbarer zu spüren. Sie stellen nationale und internationale Sicherheitsagenturen vor neue Herausforderungen – zugleich jedoch bieten geeignete Abwehrstrategien den betroffenen Gesellschaften auch bedeutsame Entwicklungsmöglichkeiten: Resiliente Nationen sind gekennzeichnet durch einen Grad an Zufriedenheit ihrer Bürger sowie deren Vertrauen in das politische und gesellschaftliche System. Verantwortungsbewusste Akteure in Regierung und Zivilgesellschaft sollten daher den engen Zusammenhang zwischen nationaler und sozialer Sicherheit berücksichtigen und danach streben, ihre Bürger zufriedener zu machen - und ihre Staaten widerstandsfähiger.

It is by no means a new phenomenon that states at war employ a broad array of instruments besides their military forces to achieve their war objectives. Deception, propaganda, information campaigns, irregular or covert operations have always been accompanying the conventional warfare through state-controlled militaries. Those measures aim to demoralize soldiers fighting at the frontline as well as to decrease the domestic support for their service. They are targeting the human psyche by raising anxieties and fears, seeding doubts, questioning the legitimacy of governments and institutions, and splitting the cohesion of a nation along social, cultural, religious or ethnic division lines.

In this regard, the hybrid warfare that the Russian Federation has been conducting in Ukraine since 2014 and the threats that it poses to other countries in its immediate or wider neighborhood do not constitute a

genuinely new concept of warfare.¹ On the contrary, in an article titled “The Value of Science in Prediction” (Ценность науки в предвидении), published in the *Military-Industrial Kurier* (военно-промышленный курьер) on 27 February 2013, Russian Chief of General Staff, Valery Gerasimov presents the uprisings of the Arab Spring and the “colored revolutions” as the results of Western strategies that show “that a perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war.”² Gerasimov also draws conclusions for future tasks of the Russian military. This article is often referred to as the Gerasimov-Doctrine that is systematically put into work in Ukraine and beyond since – which is most probably not the case.³ Gerasimov presents a Russian view on how to cope

with the perceived challenges by the West – not a blueprint for a campaign.



Fig. 1: Russian Chief of General Staff Valery Gerasimov.

However, the “use of special operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as informational actions, devices, and means” that are “constantly being perfected [...] and reflected in the doctrinal views of the world’s leading states and are being used in military conflicts”⁷⁴ is not a Western specialty. Russia intensely applied those kinds of measures in Ukraine in 2014 and since – albeit not necessarily in a doctrinal manner, but nevertheless, rather successfully. What surprised targeted states like Ukraine or the Western community at large, was less the so-called line of attack in a “non-linear war” (Gerasimov), but the degree of precision and determination to which the Russian government under Vladimir Putin arranges its military and especially its non-military operations in domains such as cyber, information technology, public opinion, diplomacy and (covert) military operations. Hereby, Russia’s initial success in Ukraine was largely due to the weakness of the country’s national cohesion, political culture and institutions, and the helplessness of the West to appropriately respond to the Russian aggression.

This helplessness has its reasons: hybrid measures are purposely applied beneath the threshold of conventional warfare. Unlike with soldiers, armored divisions or fighter aircraft crossing borders, it is

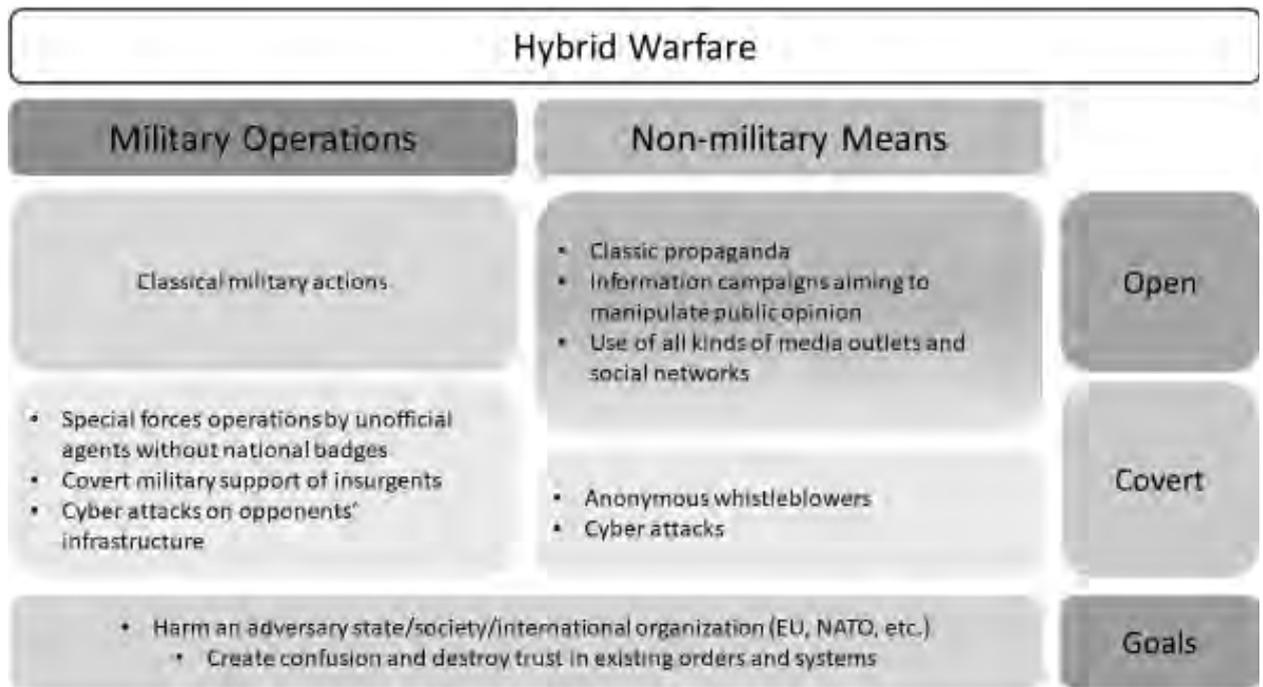
difficult to conclusively attribute, for example, a cyber-attack to an accountable actor. There are blurring borders and grey zones: is Russia supporting separatist movements in Eastern Ukraine or has it launched a military aggression against a sovereign country? Russia is part of the Normandy Format⁵ that negotiated the Minsk II agreements on a ceasefire in Eastern Ukraine but has always denied any direct involvement. It takes considerable effort to convey its narratives into Western nations and societies.

The EU, the US and other countries imposed bearable sanctions on Russia – but avoid more energetic action against Moscow since many Western countries maintain strong economic and political ties with Russia. The West maintains a unified position – but at the same time seems to tacitly accept that Crimea will not return to Ukraine in the foreseeable future. Eastern Ukraine is still war-torn while the Minsk II Agreement has not successfully been implemented.⁶

Ukraine is certainly the most important victim of hybrid warfare in Europe. Comparable threats, however, are being perceived by many countries in and around NATO and EU. Against this backdrop: what can states, societies and alliances do to defend themselves against a kind of warfare that does not strive for territorial gains or military dominance, but rather aims to destabilize if not destroy the societal order of a nation or the stability of a region? The complexity of hybrid warfare requires complex responses and a differentiated set of instruments. However, what is needed first is a thorough analysis of the nature and the functioning of hybrid threats and warfare. That includes a sober assessment of the weaknesses and vulnerabilities within states and societies that hybrid actions try to capitalize upon.

WHAT ARE HYBRID THREATS AND WARFARE?

Since 2014, the terms hybrid war or hybrid threats are in inflationary use in the current discourses on international security policy. Other than in the case of armed international conflict, however, there is no agreed definition or concept in political practice or academia that could be used to reliably qualify a situation as a hybrid war – based on which a probed set of political, military or legal measures and procedures could be invoked to cope with it. Actually, war as such can be described as hybrid because it always included dimensions beyond the mere use of military force. In that regard, the term hybrid



© Carolin Schliefersteiner

Fig. 2: This scheme illustrates measures that can be utilized in hybrid warfare.

does not add new value in the analysis of conflicts. Johann Schmid therefore proposes to focus on hybrid warfare rather than hybrid war to make clear that the same phenomenon can be viewed differently from different perspectives and in different phases of a developing conflict.⁷

Hybrid warfare can be described as a combination of the (open and covert) use of military force with any non-military means that can harm an adversary state, society or even international organizations like the EU or NATO. Other than in predominantly conventional wars where such means often complement classical military operations, they are essential instruments in hybrid warfare that often outweigh military efforts. Regarding the military, this often means special forces operations by “little green men” without national badges or covert military support of insurgents to be able to plausibly deny a direct involvement and to keep the situation as unclear as possible.

Amongst the most prominent and effective instruments in the hybrid warfare toolbox are information campaigns that aim to manipulate public opinion, damaging the adversary system’s reputation and conveying the aggressor’s own narratives of a situation and its development. In the globalized and digitalized world, such campaigns are not confined to a single target. As again the Ukrainian example shows, the 2013/14 Maidan protests against then-President Victor Yanukovich were accompanied by a massive campaign that denounced the demonstrators

and – after Yanukovich had fled the country – the new leadership as Fascists and Nazis to compromise their reputation and legitimacy and to reduce public support in Western countries.⁸ With Ukraine being only one theatre in a broader Russian hybrid campaign against Western dominance in the region, this tactic simultaneously tried to probe Western cohesion regarding common assessments of and responses to the developments in Ukraine.



© Sasha Maksymenko

Fig. 3: Protests against the Ukrainian Government in December 2014 at Kiev’s main square, the Maidan.

Information campaigns show manifold faces and use versatile channels. There is blunt propaganda and there are professionally designed networks like RT (formerly Russia Today) that is accused to present propaganda and fake news in the guise of serious information.⁹ There are troll commentators in online media, reputed experts’ comments in popular mass media and well-funded think tanks and foundations like the “Dialogue of Civilizations Research

Institute” in Berlin that help to set the agendas for public discussions.¹⁰ An old Cold War instrument is the creation of message multipliers supported financially by autochthon movements or parties that are dissatisfied with the political or socio-economic order in their countries.

The first and foremost purpose of information campaigns is to undermine public trust in the institutions, structures and procedures in the targeted states and societies, be it by fake news or by creating confusion. After the downing of Malaysian Airlines flight MH 17, Moscow presented a plethora of explanations and interpretations, many of them in partial or full contradiction to each other – simply to overwhelm the global public’s capacities for fact-based assessment and judgement of a case. The blurring borders between facts and fiction accelerate the erosion of any basis for serious debate.

Another ideal realm for hybrid warfare is the cyber space. It transcends all classical borders, it interconnects all private, public, economic or administrative areas of life and it is – despite enormous efforts by powerful states like the US, Russia or China – difficult to control. It offers convenient commodities like a globally interconnected infrastructure for real-time communication for any public, private or individual actor – thus boosting international exchange, trade and commerce. At the same time, the far-reaching dependency of all areas of life reveals increasingly existential vulnerabilities. The virtual nature of the cyber space allows all kinds of actors to launch serious attacks causing considerable damage to individuals, organizations and states at a low risk of being traced

and taken accountable. As an instrument of hybrid warfare, cyber-attacks can confuse or disrupt the communication infrastructure of states and societies, cause sectoral or temporary paralysis of public life and contribute to an overall climate of uncertainty and fear. It again can undermine the legitimacy of governments, if they are not able to protect their societies against those very real damages carried out from the virtual realm.

Attacks against the public and economic infrastructure have become every-day challenges, cyber espionage and cybercrimes pose growing threats to nations, businesses and individuals. The disclosure of hacked information about the electronic communication of prominent politicians can influence general elections, as do possible attacks on electronic voting systems. After the US presidential elections in 2016, democratic countries have to become more attentive to the perils of interferences from the cyberspace. Revelations by actors like WikiLeaks or Edward Snowden can have negative impacts on national security policies. Destructive malware like Stuxnet that allegedly was launched by the US and Israel to destroy central parts of the Iranian nuclear program has proven to be a lethal weapon in military arsenals – again without a possibility of clear attribution to an identifiable author.¹¹

HOW DO HYBRID THREATS FUNCTION?

The most important objective of hybrid warfare is to create confusion and to destroy trust in existing orders. Hereto hybrid measures aim at the basic



© WikiLeaks | David G. Stivers | Laura Poitras/Praxis Films

Fig. 4: Revelations by actors like WikiLeaks, Julian Assange (left) and Edward Snowden (right) can have impacts on national security policies or domestic politics.

features of human psyche: to feel safe and secure is a fundamental desire of every individual. This desire goes far beyond the guarantee of physical survival – human beings have the need to be respected in his or her personality, to enjoy equality and justice not only in legal terms but also in social, economic, cultural, ethnic or religious regards.

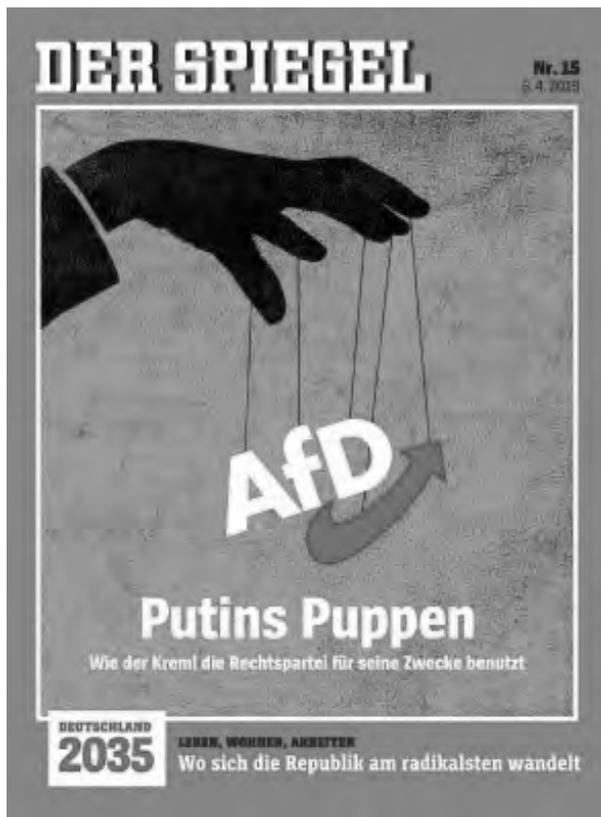
Aggregated to the level of a nation, these aspects form the foundation of the concept of societal security that guarantees fair and discrimination-free treatment to all its members. In their landmark publication, *Why States Fail* Daron Acemoğlu and James A. Robinson describe those societies as wealthy and stable that established “inclusive” political and economic institutions. Those institutions allow people to pursue their individual interests, unfold their talents and actively participate in social, economic and political life. They provide a framework for competition and consequently for development. Acemoğlu and Robinson distinguish inclusive institutions from “extractive” ones that base the well-being of certain social groups (often referred to as elites) on the exploitation and detriment of others.¹² In this perspective, a society is the more stable the more inclusive and just it is perceived by its members. Vice versa, the deeper the social splits and cleavages are, the weaker trust in institutions and the more corrupt a system is perceived, the more fragile is a society – and the more prone to hybrid intervention from outside.

The World Happiness Report of 2017 gives empirical evidence to this finding: it highlights the social foundations of happiness for individuals and nations, and its global ranking shows the close correlation between happiness and peace and societal stability.¹³ The happiest nations are the consensus-oriented ones in Scandinavia, whilst war-torn nations in Africa show the lowest degree of happiness. Acknowledging that a correlation does not necessarily indicate a causal relationship between variables, the positive impact of inclusiveness on societal security appears at least very plausible. Inclusiveness does not mean total equality. However, if social inequality is no longer accepted as the outcome of fair competition under equal conditions for all members of a society, feelings of injustice and grievances over discrimination can easily be exploited in an interplay of internal and external actors to widen the gaps along social, ethnic or religious lines. As a result, states and societies may disintegrate into antagonistic camps that are no longer able to communicate with each other –

particularly as the perception of disenfranchisement often makes those groups an easy prey for so-called strong leaders with clear-cut and simple solutions to increasingly difficult problems.

This is furthered by an important mega-trend in the use of media and information across the globe: to escape the complexity of the challenges to be dealt with, more and more people withdraw into filter bubbles that admit only those kinds of information that reinforce existing preferences, attitudes, opinions or behavior.¹⁴ To avoid cognitive dissonance, contradictory facts or deviant interpretations are actively excluded from being noticed. On the internet, the analysis of users’ search behavior is being utilized to create algorithms that propose only goods, services or information that fit into existing patterns. In political communication, agitators can plug in and reinforce dissatisfaction up to radicalization in thoughts and action.

In Ukraine, Russia capitalized upon the country’s fragile national identity, seized the opportunity of a political transition phase to carry a professionally orchestrated hybrid campaign into the country, successfully stirring up resentments amongst parts of the Russian speaking population on the Crimea and in Eastern Ukraine. It is not difficult to predict which leverage points Russia may try to use in other countries outside and within NATO or the EU. In the US and in France, the presidential campaigns 2016/17 were led against “the establishment”, in many European countries nationalist and xenophobic parties and movements have considerable success in contesting the benefits of European integration and reinforcing the internal crises of the Union. Polarization, distrust, anger, or even hatred weaken states and societies, open avenues for hybrid interference from outside, and thus constitute serious threats to national integrity and stability – within the country itself as well as with regard to regional and international orders. In April 2019, *Der Spiegel*, one of Germany’s most important weeklies, made up with a cover story on “AfD – Putin’s Puppets – How the Kremlin Employs the Right-leaning Party for its Purposes”.¹⁵ This article is a well-researched piece of investigative journalism in a top-class press medium, presenting evidence-based facts and analyses and coming to stringent conclusions. It offers a concise revelation of how external actors can capitalize upon existing grievances to deepen the cleavages within a society.



© Der Spiegel

Fig. 5: In April 2019, *Der Spiegel* made up with a cover story on “AfD - Putin’s Puppets - How the Kremlin Employs the Right-leaning Party for its Purposes”.

COUNTERING HYBRID THREATS - WHAT CAN ALLIANCES DO?

Hybrid measures often overwhelm the defense capacities of a single state and/or challenge groups of states or regions. They require concerted responses both in the field of identifying threats as well as of effectively countering them. Since hybrid threats are primarily of a non-military nature and use versatile guises and channels to unfold their impact, any alliance or security related organization must provide analytical capacities to assess, whether suspicious incidents are isolated phenomena or are indeed elements of a hybrid strategy. To this end, it is indispensable to further inter-agency exchange of data, findings and assessments to put a multitude of distinct events and cases together in a mosaic that displays a possible strategy that then can be countered. To arrange inter-agency cooperation between the military, the police, the intelligence services, the emergency management authorities and civil administrations is primarily a national task of the states. However, international organizations such as the EU or alliances such as NATO can contribute significantly to increasing the nations’ capacities.

At its summits in Wales 2014 and Warsaw 2016, NATO has brought collective defense and deterrence back into the focus of its policies. Under the headline of a “Readiness Action Plan”¹⁶, the alliance established a Very High Readiness Joint Task Force (VJTF) or took reassurance measures like the deployment of small military contingents to Estonia, Latvia, Lithuania and Poland. These Enhanced Forward Presence (EFP) deployments are designed as a show of force to a potential aggressor as well as a demonstration of the solidarity and determination of its member states.¹⁷ Partner nations like Ukraine and Georgia receive support in fields like strategy, doctrine and education, military training assistance and the (limited) provision of military equipment and non-lethal weapons. At the 2018 Brussels summit, NATO members adopted a Readiness Initiative according to which they “offer an additional 30 major naval combatants, 30 heavy or medium manoeuvre battalions, and 30 kinetic air squadrons, with enabling forces, at 30 days’ readiness or less.”¹⁸



© NATO

Fig. 6: As part of its efforts to counter hybrid challenges, NATO established a Strategic Communication Center of Excellence in Riga.

Military measures are necessary and crucial to counter the military dimension of a hybrid aggression. However, the military is only one instrument in the defense toolbox – and most probably not the one of primary importance. As part of its efforts to counter hybrid challenges, NATO established a Strategic Communication Center of Excellence in Riga (Latvia) to maintain information sovereignty and counter deception campaigns. At the Brussels summit, NATO members decided to establish Counter-Hybrid Support Teams that – upon the request of an ally – can support national efforts in a variety of areas, including cyber defense, countering disinformation or energy security.¹⁹

In response to “common threats, which can also target cross-border networks or infrastructures”, the European Union proposed a “Joint Framework on

Countering Hybrid Threats to facilitate a holistic approach that will enable the EU, in coordination with Member States, to specifically counter threats of a hybrid nature by creating synergies between all relevant instruments and fostering close cooperation between all relevant actors.”²⁰ Within this framework, the EU established institutions like the EU Hybrid Fusion Cell as an element of the EU Intelligence and Situation Centre (EU INTCEN) or the European Centre of Excellence for Countering Hybrid Threats in Helsinki (Finland)²¹ that is carried by more than twenty EU and NATO members. Those bodies do research, collect reports and assessments from member states and common agencies that can be evaluated and used to prepare national and collective countermeasures.²²

Besides its efforts within the Joint Framework, the decisive strength of the European Union lies in the social and economic basis for societal cohesion that it offers to its member states. The relatively high degree of freedom, economic opportunities, welfare, functioning institutions, rule of law and non-discrimination makes EU member states with big ethnic minorities less prone against hybrid exploitations of societal splits and cleavages. There is not much a possible aggressor can offer to outrank the tangible advantages of considerable welfare, a stable currency or an EU passport with the freedom of movement it guarantees.²³

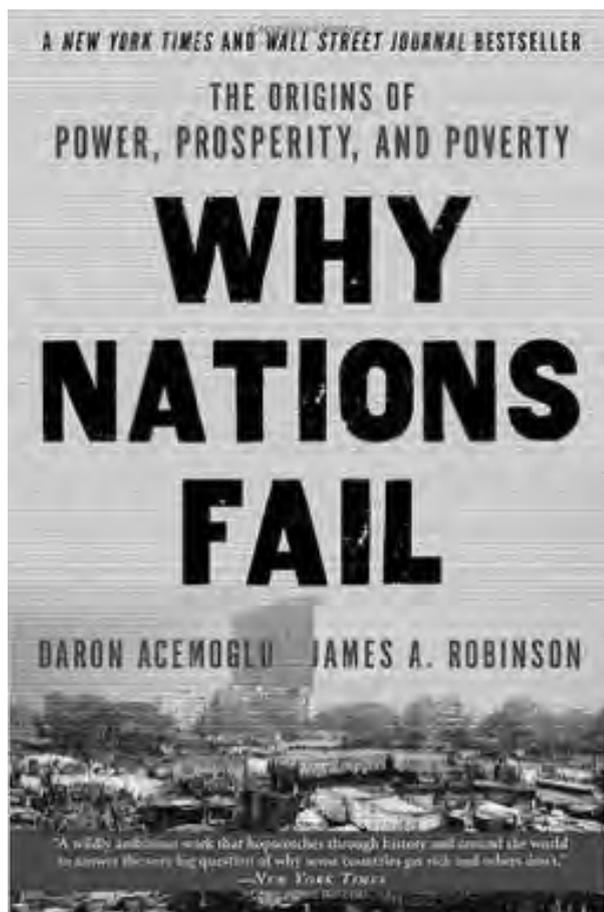
As nationalistic movements and their success in many countries illustrate, EU membership does not provide immunity against dissatisfaction that can be stirred up and exploited by interested external actors. The likelihood of those grievances to escalate to unrest or even revolution, however, seems to be limited. On the contrary, the EU provides a political and legal framework that helps to tame political actors and mitigate problematic developments in countries like Hungary or Poland where democratic achievements are currently at stake, e.g. through the rule of law framework the EU has initiated against Poland in accordance with Article 7 of the Treaty on the European Union to protect the country’s legal system.²⁴ In the case of Hungary, the European Parliament in 2018 has asked EU member states to determine, in accordance with Treaty Article 7, whether Hungary is at risk of breaching the EU’s founding values.²⁵ The jury is still out, but the sizable advantages of being part of a strong Union will outweigh nationalist temptations.

BUILDING RESILIENCE – WHAT STATES AND SOCIETIES CAN DO

In the debate on how states and societies should deal with complex hybrid risks and challenges, “resilience” has become a new key concept. As in the case of hybrid warfare, there is again no clear definition of resilience. In general terms, resilience describes the ability of a system or an organism to maintain its basic vital functions even after having suffered a severe damage.²⁶ In terms of national security, resilience means to absorb a major shock like a military strike, a terrorist or cyber-attack or a series of lower-scale actions across the whole spectrum of hybrid warfare and to continue, as far as possible, normal life. In democracies, the most important element of a nation’s or a society’s stability is its citizens’ trust in good governance and stable institutions.²⁷ To achieve and maintain this trust, it is necessary to keep the balance between security measures and freedom as well as civic rights, and to avoid a successive transformation into a surveillance state. To this end, states must create capable security agencies that are able to identify and tackle threats respectively to mitigate the consequences of hybrid attacks. To be credible, those institutions need to be strong in analysis and assessment as well as in effective counter-measures – and well interconnected with their national and international partners.

Security agencies are decisive in the struggle against hybrid threat. It is, however, equally important to any national security strategy to start from the insight that hybrid actions use and reinforce dissatisfaction and complaints within states and societies, but they do not produce or import them. Hence, building resilience begins with a remorseless analysis of a state’s weaknesses and vulnerabilities within its own realm. Governments, elites, political parties or social groups must find sober answers to the question how effectively they can guarantee societal security – or, in the terms of Acemoğlu and Robinson²⁸, how inclusive or how extractive their existing system is.

The most important indicator of inclusivity is the degree of trustworthiness that political and societal institutions enjoy amongst the citizens. It depends fundamentally on democratic legitimacy and rule of law-based procedures that guarantee integrity and transparency. This includes effective efforts to detect and fight corruption, nepotism and any other



© Crown Publishers

Fig. 7: Governments, elites, political parties or social groups must find sober answers to the question how effectively they can guarantee societal security, as Acemoglu and Robinson describe in their study.

arbitrary access to resources of power and wealth. In this context, governments and civil societies must ask themselves, whether there are equal opportunities for all citizens to participate in public, social and cultural life. Are there complaints of discrimination and how seriously are they taken? If there are cleavages and disruptions, what can be done to effectively enhance societal integration across all existing differences? It is crucial for the build-up of societal resilience how seriously the integrative efforts of a government are perceived by the individuals and groups concerned. The most important characteristic that distinguishes a mature and successful democracy from a potentially

unstable political entity is the way the majority treats minorities and respectively the manner in which the powerful treat the weak.²⁹

The way a society deals with the challenges of disinformation, fake news and propaganda can be considered as a valid litmus test of its resilience. The response to information campaigns cannot be confined to counter-propaganda or “strategic communication”. As an essential element of hybrid warfare, false information is particularly successful if political communication and public opinion are segregated in camps that live in their filter bubbles. It takes effort and time to open those people up for mutual communication and discourse on how to deal with common problems. The fundamental prerequisite for this endeavor is again trust and credibility. The less inclusive a society is, the more fertile the ground is for the manipulation of dissatisfied individuals and groups. Only if state institutions and civil societies live up to the values of free and inclusive societies based on integrity, transparency and rule of law, institutions and free media, the sharpest sword of hybrid warfare turns blunt.³⁰

CONCLUSION

Hybrid threats and warfare are not new phenomena, but in the globalized world with its breath-taking development of ever-faster communication, its impacts become massive and dangerous. They pose new challenges to national security policies and agencies – but at the same time adequate defensive measures open immense opportunities for a society: true resilience requires a certain degree of satisfaction and happiness amongst all its citizens. Responsible governments and civil society actors will take into account the close nexus of societal and national security and strive to make their citizens happier – and their nations stronger.

ENDNOTES

- ¹ Regarding the development of the term “hybrid war” see Frank G. Hoffmann, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA 2007). Online: http://www.projectwhitehorse.com/pdfs/HybridWar_0108.pdf. Wolfgang Schreiber, *Der neue unsichtbare Krieg? Zum Begriff der „hybriden“ Kriegsführung*, in: *Aus Politik und Zeitgeschichte* 66, No. 35-36 (2016), 11-15. Online: <http://www.bpb.de/shop/zeitschriften/apuz/232975/moderne-kriegsfuehrung>.
- ² Valery Gerasimov, *The Value of Science in Prediction (Ценность науки в предвидении)*, in: *The Military-Industrial Kurier (военно-промышленный курьер)* No. 476, 27.2.2013. Original online: https://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf. The quotes of the Gerasimov paper are taken from the translation of the article provided by Robert Coalson and published in the Huffington Post. Online: https://www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine_b_5748480.html.

- ³ In a Foreign Policy article of 5 March 2018 titled “I’m Sorry for Creating the Gerasimov Doctrine”, Mark Galeotti, who claims to have coined that term, writes that such a doctrine does not exist and regrets that term is widely being used in a flawed manner as it might mislead Western responses to the Russian proceedings. Online: <https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/>.
- ⁴ Gerasimov, Value.
- ⁵ The Normandy Format is an informal negotiation forum on the situation in Eastern Ukraine. It is named after a meeting of German Federal Chancellor Angela Merkel, French President François Hollande, Russian President Vladimir Putin and the Ukrainian President Petro Poroshenko during the celebrations of the 70th anniversary of the Allied landing in the Normandy on 6 June 1944.
- ⁶ The Minsk II agreement was signed on 12 February 2015 by the OSCE-led Trilateral Contact Group after long negotiations between the protagonists of the Normandy Format, Hollande, Merkel, Poroshenko and Putin in the capital of Belarus as an attempt to halt the ongoing violence in the east of Ukraine. Full text of the “Package of Measures for the Implementation of the Minsk Agreements” and “Declaration of the President of the Russian Federation, the President of Ukraine, the President of the French Republic and the Chancellor of the Federal Republic of Germany in support of the ‘Package of Measures for the Implementation of the Minsk Agreements’, adopted on 12 February 2015 in Minsk”. <https://www.un.org/press/en/2015/sc11785.doc.htm>. It stipulated the conditions of a ceasefire, its monitoring by the OSCE, the full control of the state border through Ukraine and constitutional reforms granting a “status of certain areas of the Donetsk and Luhansk regions” (Paragraph 11). The implementation of the Minsk II agreement failed thus far, not least due to the demand of constitutional changes that would require a two-thirds majority in the Ukrainian parliament. The situation in Eastern Ukraine has become a protracted conflict with little likelihood for settlement in the foreseeable future. Regarding the debate on Minsk II see <https://carnegieeurope.eu/strategieurope/?fa=68084>.
- ⁷ Johann Schmid, *Hybride Kriegsführung* (working title), in: Stephan Böckenförde, Sven Bernhard Gareis (eds.), *Deutsche Sicherheitspolitik*. 3rd edition (Leverkusen-Berlin-Toronto 2019).
- ⁸ See Vladimir Sazonov, Kristiina Müür, Holger Mölder (eds.), *Russian Information Campaign against the Ukrainian State and Defence Forces* (Tartu 2015). Online: https://www.ksk.edu.ee/wp-content/uploads/2017/02/Report_infoops_08.02.2017.pdf.
- ⁹ See: *Die Zeit*, 19.11.2014. Online: <https://www.zeit.de/politik/ausland/2014-11/rt-deutsch-russland-propaganda-luegen>.
- ¹⁰ The Centre was established in Berlin in 2016 and is being led by Vladimir Jakunin, the former CEO of Russian Railways, a close associate of Russian President Putin. See: <https://www.dw.com/en/putin-associate-opens-russia-friendly-think-tank-in-berlin/a-19372110>.
- ¹¹ Sean Collins, Stephen McCombie, *Stuxnet: the emergence of a new cyber weapon and its implications*, in: *Journal of Policing, Intelligence and Counter Terrorism* 7, No. 1 (2012), 80-91.
- ¹² Daron Acemoglu, James A. Robinson, *Why Nations Fail: The Origins of Power, Prosperity, and Poverty* (London 2013).
- ¹³ The World Happiness Report is produced yearly by the United Nations Sustainable Development Solutions Network in partnership with the Ernesto Illy Foundation and other partners. It ranks more than 150 countries based on the life evaluations of their inhabitants. Online: <https://worldhappiness.report/ed/2017/>.
- ¹⁴ The term “filter bubble” was coined by Eli Pariser in his book *The Filter Bubble – What the Internet is Hiding from You* (London 2011). See also Dominic Spohr, *Fake news and ideological polarization: Filter bubbles and selective exposure on social media*, in: *Business Information Review* 34, No. 3 (2017), 150-160. Seth Flaxman, Sharad Goel, Justin M. Rao, *Filter Bubbles, Echo Chambers, and Online News Consumption*, in: *Public Opinion Quarterly* 80 (2016), Special Issue, 298-320. Online: <http://dx.doi.org/10.2139/ssrn.2363701>.
- ¹⁵ For an overview, see Annegret Bendiek, *European Cyber Security Policy*. SWP Research Paper 13 (Berlin 2012). Online: <https://www.swp-berlin.org/en/publication/european-cyber-security-policy/> and the dossier on digitalisation and cyber security. Online: <https://www.swp-berlin.org/en/dossiers/digitalisation-cyber/cyber-security/>.
- ¹⁶ NATO, *Wales Summit Declaration* (2016), Paragraph 5-13. Online: https://www.nato.int/cps/en/natohq/official_texts_112964.htm#rap. For an overview see: *NATO’s Readiness Action Plan*. Online: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-rap-en.pdf.
- ¹⁷ NATO, *Warsaw Summit Communiqué* (2016), paragraph 40. Online: https://www.nato.int/cps/en/natohq/official_texts_133169.htm#rap.
- ¹⁸ NATO, *Brussels Summit Declaration* (2018), Paragraph 14. Online: https://www.nato.int/cps/en/natohq/official_texts_156624.htm#21.
- ¹⁹ *Ibid.*, Paragraph 21.
- ²⁰ European Commission, *Joint Framework on countering hybrid threats, a European Union response*. Joint Communication to the European parliament and the Council. Of 6 April 2016. Online: <file:///C:/Users/drsve/OneDrive/Dokumente/Forschungsthemen/Hybrid%20Warfare/EU%20Joint%20Communication.pdf>, 2f. www.hybridcoe.fi.
- ²¹ For an overview of EU activities see: *EU External Action Service, A Europe that Protects*. Brussels Online 2018. https://eeas.europa.eu/sites/eeas/files/hybrid_threats_en_final.pdf.
- ²² It can be discussed, whether the United Kingdom’s retreat from the EU (BREXIT) can be considered as a counter-argument to the Union’s ability to provide a stable and cohesive framework for its member states. Without doubt, the BREXIT has its causes in the dissatisfaction of large parts of UK’s population with the transfer of national sovereign rights to the EU. The promised objective was the restitution of British sovereignty and grandeur. Other than in the case of Ukraine or – possibly – in other Eastern EU countries, however, the BREXIT was not motivated by an external intervention to spur resentments of an ethnic minority against the majority and raise sympathies for a “mother nation”.
- ²³ For an overview and further links see: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/effective-justice/rule-law/rule-law-framework_en.
- ²⁴ Original title: *AfD – Putins Puppen*. *Wie der Kreml die Rechtspartei für seine Zwecke benutzt*, in: *Der Spiegel* No. 15, 6.4.2019.
- ²⁵ The American Psychological Association defines resilience as “the process of adapting well in the face of adversity, trauma, tragedy, threats or significant sources of stress – such as family and relationship problems, serious health problems or workplace and financial stressors. It means ‘bouncing back’ from difficult experiences.” Online: <https://www.apa.org/helpcenter/road>

resilience. In social and political science this term has been adopted to describe the ability of a state or a society to carry on at the greatest possible degree of normalcy during or after grave stress situations such as natural disasters, terrorist assaults or armed attacks.

²⁷ See: International Institute for Democracy and Electoral Assistance (IDEA), *The Global State of Democracy. Exploring Democracy's Resilience* (Stockholm 2017). Online: <https://www.idea.int/g sod/>.

²⁸ See Endnote 12.

²⁹ See Endnote 27, Chapter 2. *Democracy's resilience in a changing world*.

³⁰ See *World Happiness Report 2019*, 55f.

LIST OF FIGURES

The illustrations for this article have been selected by the JIPPS editorial committee.

Fig. 1 Photo: Kremlin.ru, [https://commons.wikimedia.org/wiki/File:Valery_Gerasimov_\(2015-05-12\).jpg](https://commons.wikimedia.org/wiki/File:Valery_Gerasimov_(2015-05-12).jpg).

Fig. 2 Graphic: designed by Carolin Schlieffsteiner for JIPSS.

Fig. 3 Photo: Sasha Maksymenko, CC BY 2.0, via Wikimedia Commons, [https://commons.wikimedia.org/wiki/File:Anti-government_protests_in_Kiev_\(13087792943\).jpg](https://commons.wikimedia.org/wiki/File:Anti-government_protests_in_Kiev_(13087792943).jpg).

Fig. 4 Logo: WikiLeaks.

Photo: by David G. Silvers, CC BY-SA 2.0, via Wikimedia Commons, https://commons.wikimedia.org/wiki/File:Julian_Assange_August_2014.jpg.

Photo: Laura Poitras/Praxis Films, CC BY 3.0, via Wikimedia Commons, https://commons.wikimedia.org/wiki/File:Edward_Snowden.jpg.

Fig. 5 Cover: *Der Spiegel* No. 15/2019.

Fig. 6 Logo: NATO Strategic Communication Center of Excellence.

Fig. 7 Cover: copyright Crown Publishers.