Teka Komisji Prawniczej PAN Oddział w Lublinie, vol. XIV, 2021, no. 2, pp. 91–100
https://doi.org/10.32084/tekapr.2021.14.2-8

HYBRID THREATS – MEANS OF DESTABILIZATION OF LAW AND ORDER IN MODERN DEMOCRATICS SOCIETES. IDEA AND METHODOLOGY OF PROPOSED RESEARCH

Dr. habil. Paweł Chodak, University Professor

AGH University of Science and Technology in Kraków, Poland
e-mail: pchodak@agh.edu.pl; https://orcid.org/0000-0003-3557-4648

Dr. Krzysztof Krassowski

AGH University of Science and Technology in Kraków, Poland
e-mail: kkr@agh.edu.pl; https://orcid.org/0000-0002-4989-0804

Dr. Tomasz Wierzchowski

AGH University of Science and Technology in Kraków, Poland
e-mail: tomwie@agh.edu.pl; https://orcid.org/0000-0002-3986-8187

Abstract. Threats are one of the most serious threats to the legal order of a democratic state. Their non-linear, asymmetric nature makes them more dangerous than other threats to the legal order. The use of multifaceted measures as a weapon disrupts, above all, the legal order of the state. Hybrid threats rely heavily on non-military domains. Civilian populations are central to the hybrid threat scenarios as sources for potential socio-political vulnerabilities and as targets for non-military threats and attacks, not least disinformation campaigns. A significant part of the hybrid threat phenomena is psychological. Actors targeting communities/societies to exacerbate weaknesses do not necessarily create social vulnerabilities themselves but make use of divisions that already exist in civil society. Using disinformation, populations are targeted and used as potential weapons within the state/society in question. This paper shows a concrete scientific approach to the study to of this issue.

Keywords: hybrid threats, law, security, information, democracy, state

INTRODUCTION

Hybrid threats is one of the most crucial issues confronting contemporary democratic societies and heavily impacting rule of law. Potential future crises in Europe and globally will be dominated by a complex, hybrid form of challenges that target populations, in turn creating instability [Major and Mölling

2015; O'Loughlin 2015; Giegerich 2016]. Perception for rule of law, citizen trust, loyalties, values, and politics are central to understanding these challenges to stability. Sustainable and legitimate governance relies upon trust between government institutions enforcing rule of law and their citizens, and sustainable government is weakened if trust is weak. Destabilization, characterized by the purposeful use of primarily non-violent means, results from the reduced trust, beyond the healthy skepticism of an informed populace, between citizens and the state [Gashi and Maqedonci 2017; Cusumano and Corbe 2017].

Though there is no agreed definition of hybrid threats, we can characterize its main features, as: 1) an amalgam of multiple means including military, political, economic, legal, cultural, social, infrastructure, cyber and information domains; 2) a hostile actor aims to avoid detection and tries to diffuse/ confuse the situational awareness; 3) a hostile actor can be state, nonstate or proxy actors, or all of them; 4) creation of a situation where existing societal differences and grievances are consciously exacerbated, causing public harm. This is especially done by mixing information with intentional disinformation, through the distribution of misleading or fake news on already contentious social issues (e.g. migration); 5) structural breaking of the rule of law in order for hostile takeover of social resources (e.g. voters), material resources, diminishing democratic process, or even questioning independence of a given territory (e.g. case of Crimea).

1. RESEARCH IDEA

Hybrid threats rely heavily on non-military domains. Civilian populations are central to the hybrid threat scenarios as sources for potential socio-political vulnerabilities and as targets for non-military threats and attacks, not least disinformation campaigns. While misinforming others might be unintentional, the intentional act of misinforming someone constitutes disinformation, defined as "verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm".[1]

A significant part of the hybrid threat phenomena is psychological. Actors targeting communities/societies to exacerbate weaknesses do not necessarily create social vulnerabilities themselves but make use of divisions that already exist in civil society. Using disinformation, populations are targeted and used

[1] Joint Communication to the European Parliament and the Council: A Strategic Approach to Resilience in the EU's external action. High Representative of the Union for Foreign Affairs and Security Policy: European Union, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52017JC0021 [accessed: 19.11.2021].

as potential weapons within the state/society in question. Inequalities within a society can be used to exacerbate dissatisfaction to the advantage of an enemy that wishes to create an unstable environment. The resulting insecurity can increase mistrust in society [Roell 2016].

While cooperation between civilian and military authorities or organizations is assumed, this approach takes little account of the general population. Who are "we" today? Would we respond to a crisis together? Or would we be fragmented according to our sense of belonging to the interests of our community or the state? The delivery of "preparedness" brochures in some countries of the world attempts to mitigate insecurity amongst civilians, as well as control the civilian response, to guide it as much as possible through civilian authorities to ensure that civilian responses are predictable and unified.

To assume such unity within the civilian population can be problematic, however. In a podcast broadcasting a roundtable session at the annual Chatham House London Conference,[2] participants discussed the disconnect between governments and their populaces, the rise of populism and rejection of elites fostering destabilization, and the challenges of reconnecting political processes to the everyday concerns of average people. It is increasingly clear that we still lack understanding about the civilian landscape that is and will continue to be a target for possible disinformation but is also potentially a center of gravity for conflict resolution.

Trust processes and levels between the governed and government need re-examination. Having a better understanding of where the potential vulnerabilities lie within possible target societies enables these same societies – and the diverse civilians within them – to develop measures that can build trust and solidarity within them, making them less vulnerable to destabilization. Disinformation/propagation of fear of certain groups of people with the purpose of destabilizing a society are understood as hybrid threats, however we want to better understand how this is a hybrid threat, and how to mitigate it, if and when necessary. Disinformation has gained increasing attention as a feature of hybrid warfare which employs military and non-military tools to destabilize a society [Reichborn–Kjennerud and Cullen 2016]. There is still a gap however in how these threats can and should be understood in hybrid contexts, including how emotions like fear or anger, which are difficult to measure or control, resulting from disinformation become threats in and of themselves. What are we missing before emotions become grievances expressed as nationalist/religious populism or extremism?

When it comes to malicious or criminal acts in cyberspace – from attacking critical infrastructure to disseminating false or misleading information – it has been noted that one long-term impact might be social discontent and unrest,

[2] See *How Can Political Elites Reconnect with Voters?* Undercurrents. A. Frimston and B. Horton, Chatham House, London (29 June 2018).

including the loss of public confidence in the government, even if the actual damage caused by the cyber-criminal activities was minimal [Choo 2011]. How does disinformation become a threat and what can be done to enhance societal trust as a response? Societal trust is a key target for destabilization, which in turn affects civilian capabilities during a crisis or conflict.[3] The potential for insecurity increases as societal trust decreases [Bilgic 2013]. From previous conflicts (from WWII Europe to former Yugoslavia, Afghanistan, Iraq, Georgia, Ukraine and Syria) we know that civilians have influenced the direction and nature of security/insecurity [Hoogensen 2014]. Both national and multilateral institutions (NATO/EU) are either developing or reviving defense systems that combine both military and civilian efforts [Shea 2016]. There is nevertheless a significant research and practical gap in knowledge regarding how, and to what extent, societal trust and civilian capabilities can affect institutional planning, preparedness, and responses to emerging crisis situations, and through which mechanisms, in particular to threats in hybrid warfare scenarios.

The research is required paying attention to military and civilian authorities' role in combating hybrid threats but puts a hitherto neglected focus on the effects that disinformation has on civilian agency (capabilities) in the evolution of a crisis or conflict. Civilian agency is generally understood as the capacities of individual citizens as well as civil society and its organizations at large. It is not fully understood how civilian capacities are influenced during crises, and how different authorities coordinate their action in this rather new hybrid security field. We should ask: How does civilian agency affect societal trust – crucial to cooperation and security – in the face of hybrid threats to security? We should examine these threats which appear intangible but have high trigger responses amongst civilians, affecting civilian capabilities.

The scientific problem raised is a socio-political-legal question, that asks how we can understand people's actions and reactions in crisis better. To answer this, however, needs more than one conduit to knowledge. We need to know more about people's reactions in crisis (security studies including cybersecurity, media studies, sociology, social psychology) as well as how states have prepared for and control people's actions and behaviors through law and order (law, societal security policy). But the relationship between civilians and their government agencies during a crisis remains unclear. It is often taken for granted that civilians are the passive element in crisis, following the lead of authorities, but research from other conflict settings (outside of Europe) demonstrate this is not the case [Parashar 2016; Hoogensen 2014].

[3] See Støtte og samarbeid: En beskrivelse av totalforsvaret i dag (Support and Cooperation: A description of total defence today), Department of Defence/Department of Justice and Preparedness, Oslo 2015.

The overall goal is to improve societal level abilities to manage crises (where hostile actor is irrelevant or difficult to determine) and conflicts (identifiable hostile counterpart), as well as expand possibilities for open dialogue for civilians.

The primary ambition should be to increase research-based knowledge about the role of civilians and civilian agency – what people do – in crisis and conflict, that are also in accordance with legal obligations. Increased knowledge on civilian agency in relation to trust during times of destabilization or crisis will assist both civilian and state actors to mitigate vulnerability and increase the scope of non-militarized solutions to conflict.

The innovative in the emphasis on interdisciplinary "bottom up" methodologies (intersectionality) applied to law and societal security, which have otherwise been heavily approached by "top-down," state-centric focus. Such state-centric approaches are nevertheless not ignored, as authorities play an important role also from the societal security perspective. Thus we should cooperate heavily with relevant end users who can benefit immediately from the ongoing research and at the same time provide important information, to authorities, private actors (e.g. critical infrastructure operators), and civil society organizations, while at the same time maintaining our focus on citizens to inform us, guide us through our research (open lectures/debates), and receive results.

2. RESEARCH METHODOLOGY AND MILESTONES

Objective 1: Investigation of the current state-of-the-art. A thorough literature review should be performed at the start of the research, with ongoing literature review as needed. The review will identify the best methods available for achieving other project objectives.

Objective 2: Development of fundamental conceptual framework. Since there are no commonly agreed definitions of basic concepts, including but not limited to, "hybrid threats" and "disinformation," research will be performed on both national and international basis in order to develop common conceptual system, taking into account specificity of Poland and CEE countries. It shall enable common understanding and scope of researched data sets – prerequisites for proper comparative analysis, as well as provide contribution to theoretical concept framework.

Objective 3: Provision of novel theoretical scientific contribution. Within scholarly rich environment, the research will develop "bottom-up" – grounded (civilian-oriented), innovative theoretical contributions on societal trust research and the impact of civilian agency on destabilization or crisis/conflict scenarios, without omitting the more traditional state-centered approaches.

Objective 4: Contribution to the development of legal regulations, policies, interventions and doctrines. The research will provide contribution to development of laws, policies, interventions and doctrines relevant to human and societal security planning – especially focusing on resilience strategies of trust, taking into consideration legal obligations of the state and maximization of civilian capacities and nonmilitary responses to threat scenarios. The empirical data gathered will also provide a solid basis for further research on the complex relations between civilians and authorities during crises.

Objective 5: Open engagement with society. To this end, the research will ensure its relevance and benefit to society, as well as inclusion of civil society actors, through open public debate of draft project deliverables including, but not limited to, public evaluation of proposed theoretical framework, possible absorption of research results and in particular making visible different threat perceptions in particular counties. Most importantly, this research has as an objective aim to increase trust between people and their authorities and increase knowledge about non-militarized solutions to conflicts.

Objective 6: Based on the ready-to-use web crawlers developed at Forensic Software Laboratory or Cybersecurity Centre a dedicated service will be developed, focused on finding texts (e.g. blog posts, tweets etc) which may be perceived as traces of hybrid threat. This search will be encoded following the knowledge on discovering the hybrid threats and know-how related to Natural Language Processing will be utilized in order to implement components of this web crawler. The prototype of the constructed software solution will be made available on the web and configured to work on selected, popular information and blog services, Twitter etc.

Objective 7: Knowledge-building and dissemination. Research results will be presented at conferences and published in proceedings and journals, with contributions in pop-sci media if appropriate. Deliverables and resources will be made publicly available as far as possible.

To better understand the civilian landscape, it is crucial to understand the various positions or identities within civilian communities that can be vulnerable or resistant to threats of disinformation. Identity plays a crucial role in trust. Intersectionality focuses on the experiences of individuals/civilians, and how identities shape experiences including fear, anger, belonging, etc. It finds its roots in a critique of feminist approaches that were insensitive or blind to the different experiences of women on the basis of race, class, orientation, ethnicity, and other markers of positionality that impacted their power and agency. Coined by Kimberlé Crenshaw in the late 1980s [Crenshaw 1991], the term "intersectionality" was designed to critically assess the intersection between race and gender, and at its core has a "nonpositivistic, non-essentialist understanding of differences among people as produced in on-going, context-specific social processes" [Marfelt 2016, 32]. As such, intersectionality is an important analytical tool when examining the power dynamics of civilians in relation to the creation/maintenance/strengthening of trust in a society, and in relation to the articulations of state actors who have a particular influence on how trust is understood and perpetuated socially.

Intersectionality infuses research approaches in two ways. Establishing an interdisciplinary "checklist" of questions we need to ask while designing our respective research methods – asking what assumptions of power and identity are made about the populations we are investigating both within our methods as well as the sources of data we explore (ie: current law and legal documents). Thereafter we will investigate cases by gathering data and empirical evidence via intersectionality-informed quantitative and qualitative methods including surveys (EUSurvey) and semi-structured interviews with civilians and civil societies, and document analysis of laws, white papers and political strategies.

This includes examining disinformation, different hybrid threat methods and motivations, and target groups utilizing comparative analysis, content analysis, statistical analysis, interdependency analysis, among others. The methods and tools will include textual and audio-visual document studies, in-depth interviews, targeted social media and media observations and data gathering, large-n online surveys among NGOs, citizen cafés, and, when possible, participating observation and small-scale experimental tabletop tests. We further apply the modified positivist approach, assessing the relevant domestic and international legal regulations (eg. International agreements and international customary law), complementing with additional arguments sought in case law and legal literature. The research on emergency laws will be undertaken in the doctrinal tradition. The collected data with thereafter be triangulated and assessed again through intersectional lenses that both unpack and expose our data according to the way various identities are created, changed, or distorted, as well as present possible solutions to maintaining societal integrity (stability) while allowing for diverse identities.

All the aforementioned Tasks will be performed in parallel within all three established Research Areas, that together constitute a comprehensive interdisciplinary research project:

3. PROPOSED RESEARCH AREAS

3.1. Research Area 1 – Social Science perspectives

The task will address the question of societal trust. In a preparatory literature review, the research will critically determine what precisely trust is and how it functions in democracies. Is trust always a good thing? Or, might there be good reasons to embrace a certain dose of distrust as a sign for functioning democracy? Researchers will inquire into the sources of contemporary distrust in state institutions. Through initial surveys, relevant candidates for in-depth qualitative interviews will be identified. Intersectional lenses will be applied throughout selection. Informants will be interviewed twice during the project to address possible changes over time and through our scholarly engagement. Main hypothesis is that potential growing distrust has a multiplicity of reasons intertwined with identities, many of them home-grown. The second issue that will be addressed is threat perception and the formation in contemporary commercial and noncommercial social media. Recently, economic incentives and algorithmic trajectories have been identified as main drivers of radicalization and distrust in digital environments [Fuchs 2017]. Through quantitative assessments and qualitative content analyses of social media content, the research will: a) map what content exists and how certain profiles and sites connect, b) qualitative interviews will assess how users react to content received and why certain items are passed on before, c) identities, technological logics and economic incentives will be connected to the data and a comprehensive picture of contemporary socio-technical networks will be drawn up.

Main hypothesis is that technological and economic factors constitute tacit frames for civilian agency that privilege radicalizing and distrusting content. The third issue is susceptibility of society to digital threats in general and disinformation in particular, including relevant assessment of present standing of society in general and impact of demographics. Research should provide answers to number of questions related to e.g. current common values shared by society, information sphere, cultural awareness, or lack of it. Analysis and evaluation of common social values that are most endangered by hybrid threats is a prerequisite for correct determination of dangers posed by threats. Proposed research should not only identify such values and categorize them, but also reveal strongest and weakest elements. Analysis regarding social consciousness of threats in question should be also conducted, in particular in CEE context and new phenomena – immigration and expansion of Islam, military and terrorist threats. A map of topography of information impact on society should be taken into account in research program too.

3.2. Research Area 2 – Societal security/technological perspectives

This task will address cyber space as a forum of social action, having its own rules however which are not always regulated. What are the technological elements that make civil societies, or individual citizens, and through them democratic societies, especially vulnerable for malicious efforts to destabilize the traditional democratic order? Does, and if so, how does, identity play a role in these efforts? What are the defensive strategies, technological and non-technological, that can be used again this? The second issue that will be addressed concerns reactions of civil society and citizens in light of attacks disrupting critical infrastructure and vital societal functions embedded in it, such as information, transport, electricity, water, health care, emergency services and so forth. How do we understand "resilience" in these cases, and what is the tolerance and societal resilience level of the society and its citizens? Does resilience change according to identity markers (gender, race, ethnicity, socio-economic class, etc)? How does technology address this threat, by enabling and/or limiting it? Analysis and evaluation of susceptibility of e-space to cyber and electronic threats, will be also undertaken in context of vulnerability to particular hybrid threats identified.

3.3. Research Area 3 – Legal perspectives

This task will address the issue of legal possibilities and limitations for the state in protecting societal security and maintaining/building/rebuilding trust in the face of cyberattacks of a non-military character. Such interference may be undertaken by a government (e.g. espionage, propaganda, or more subtle disinformation operations in order to influence an election), or by private, non-state entities (e.g. industrial espionage or political opposition groups). The second issue that will be addressed concerns legal responses to non-military intervention in the internal affairs of a state by (a) foreign state(s) or non-state entities, with a special focus on hybrid threats. Clarity regarding legal and efficient responses, including what kind of intervention is legal under international law, and which responses thereto may the target state legally undertake, alone or in concert with other states. Emphasis will be placed on how the law recognizes the ways in which different population groups may be targeted based on specific identities, and how law can mitigate this. Assessment of current shape and state of regulations enabling and supporting fight with hybrid threats will be dedicated to evaluation of present and future of regulations governing public security issues, in particular relevant to protection of citizen rights in fight with threats of hybrid nature. RA1 and RA2 will inform this particular RA with civilian (bottom-up) and technological perspectives that need to be taken account by law.

The safety of respondents and the research team for each case study is paramount and will guide all research decisions. Protecting confidentiality is essential to ensure both informants' safety and data quality. Ethical guidelines insist on elaborate procedures for procuring informed consent and assuring the voluntariness of the participation so participants will not become mere "objects" of study.

Fundamental issues shaping modern societies, especially the ones of Western democracy type, are being addressed, going beyond mere multidisciplinary by combining the different perspectives into a holistic, intersectional analysis, performed in the context of comparative research providing selected national perspectives. Proposed research evaluated in the present paper is innovative in its focus on both the state and civilian levels in studying hybrid threats and how they interact together, and it takes into account fundamental issues of various paths of development of democracy in Europe. Research outcomes, therefore, might be appreciated by different communities in Social Sciences, Humanities and Computer Sciences.

REFERENCES

Bilgic, Ali. 2013. "Trust in world politics: converting «identity» into a source of security through trustlearning." *Australian Journal of International Affairs* 68, no. 1:36–51.

Choo, Kim-Kwang R. 2011. "The cyber threat landscape: Challenges and future research directions." *Computers & Security* 30:719–31.

Crenshaw, Kimberle. 1991. "Mapping the Margins: Intersectionality, Identity Politics, and Violence Against Women of Color." *Stanford Law Review* 43 (6):1241–299.

Cusumano, Eugenio, and Marian Corbe, eds. 2017. *A Civil-Military Response to Hybrid Threats*. London–New York–Shanghai: Palgrave Macmillan.

Fuchs, Christian. 2017. *Social Media: A Critical Introduction*. 2nd edition. London: Routledge.

Gashi, Bejtush, and Ejup Maqedonci. 2017. "Hybrid Threats – Global Challenge of Modern Times." *Polemos* 20, no. 1–2:91–102.

Giegerich, Bastian. 2016. "Hybrid Warfare and the Changing Character of Conflict." *Connections: The Quarterly Journal* 15, no. 2:65–72.

Hoogensen, Gjørv, G. 2014. *Understanding Civil-Military Interaction:Lessons Learned from the Norwegian Model*. Military Strategy and Operational Art series. London: Ashgate Publishers.

Major, Claudia, and Christian Mölling. 2015. "A Hybrid Security Policy for Europe: Resilience, Deterrence, and Defence as Leitmotifs." *Stiftung Wissenschaft und Politik* 22:1–4.

Marfelt, Mikkel M. 2016. "Grounded Intersectionality: Key Tensions, a Methodological Framework, and Implications for Diversity Research." *Equality, Diversity and Inclusion* 35, no.1:31–47.

O'Loughlin, Ben. 2015. "The permanent campaign." *Media, War & Conflict* 8, no. 2:169–71.

Parashar, Swati. 2016. "(En)Gendering the Maoist Insurgency in India: Between Rhetoric and Reality." *Postcolonial Studies* 19, no. 4:445–62.

Reichborn–Kjennerud, Erik, and Patrick Cullen. 2016. *What is Hybrid Warfare?* Policy Brief. Oslo: Norwegian Institute of International Affairs.

Roell, Peter. 2016. "Migration – A New Form of «Hybrid Warfare»?" *ISPSW Strategy Series: Focus on Defence and International Security* 422:1–7.

Shea, Jamie. 2016. "Resilience: a core element of collective defence." *NATO Review*, 30.03.16. https://www.nato.int/docu/review/articles/2016/03/30/resilience-a-core-element-of-collective-defence/index.html [accessed: 19.11.2021].