Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

I.M. Pascu & N.-S. Vintila,
Connections QJ 19, no. 3 (2020): 55-66
https://doi.org/10.11610/Connections.19.3.04

Research Article

Strengthening the Resilience of Political Institutions and Processes: A Framework of Analysis

Ioan Mircea Pascu and Nicolae-Sergiu Vintila

Abstract: Conventional as well as atypical threats and vulnerabilities tend to undermine the core principles and functioning mechanisms of democratic societies. This article examines internal weaknesses and foreign intervention operations seeking the manipulation of the electorate and thus diminishing legitimate political participation and questioning the very essence of democracy. The analytical focus is on manipulation and disinformation mainly through mass media and social network platforms. This is increasing the risk of undermining public confidence and trust in democratic institutions and processes. The main argument is that democratic institutions and processes can and must be made more resilient. The article provides a framework of analysis for the resilience of political institutions and processes and investigates current initiatives, including of EU and NATO, to strengthen resilience.

Keywords: resilience, democratic resilience, disinformation, computational propaganda, post-truth, sharp power, democracy, foreign influence operations.

> *Democracy itself is under assault from foreign governments and internal threats, such that democratic institutions may not flourish unless social data science puts our existing knowledge and theories about politics, public opinion, and political communication to work. These threats are current and urgent, and, if not understood and addressed in an agile manner, will further undermine European democracies.*[1]

[1] Samuel C.Woolley and Philip N. Howard, eds., *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, Oxford Studies in Digital Politics (Oxford: Oxford University Press, 2018), p. 245. https://doi.org/10.1093/oso/9780190931407.001.0001.

The "end of history" as announced by Francis Fukuyama[2] three decades ago has certainly ended. This is a sobering time for the dream of the inevitable advance of liberal democracy. Analysts, liberals, and rivals alike agree that democracy is "in recession,"[3] "in retreat,"[4] that the international liberal, rules-based order, is at least fracturing if not dissipating altogether.

Our working hypothesis and the core argument of this article is that democratic institutions and processes can and must be made more resilient both to extreme political events and crises *and* to "normal emergencies." The article analyses *political resilience*, meaning saving democracy, and keeping it clean. We will focus on a limited number of challenges, in particular on the *manipulation of the electorate*—making someone vote against his or her initial intention—thus *diminishing legitimate political participation and undermining public confidence and trust in democratic institutions and processes*. The analytical focus will be on manipulation and misinformation conducted mainly through mass media and social network platforms.

Bolstering the resilience of democratic institutions and processes is a topic that has increased importance due to the fact that challenges are coming not only from the *growing fragility of liberal democracy* and from domestic political actors but often result from *foreign political influence operations* and even state-sponsored operations against NATO and EU member states (increasingly including cyber espionage, direct interference in electoral processes, critical infrastructure vulnerability scanning, disruptive attacks, as well as propaganda and disinformation campaigns[5]). These operations represent a *serious security threat to our societies*.[6]

Trust in political institutions and processes, in particular electoral participation, is a key indicator of the viability and legitimacy of democracy. It should be seen in correlation with other critical challenges and threats to established as well as newer democracies as the abuse of executive power, corruption and

---

2 Francis Fukuyama, "The End of History?" *The National Interest*, no. 16 (Summer 1989): 3-18.

3 Larry Diamond, "The Democratic Rollback. The Resurgence of the Predatory State," *Foreign Affairs* 87, no. 2 (March/April 2008): 36-48.

4 Freedom House, *Democracy in Retreat: Freedom in the World 2019* (Washington, DC: Freedom House, 2019), https://freedomhouse.org/sites/default/files/Feb2019_FH_FITW_2019_Report_ForWeb-compressed.pdf.

5 Patryk Pawlak, "Horizontal Issues," in *After the EU Global Strategy – Building Resilience*, ed. Florence Gaub and Nicu Popescu (Paris: European Union, Institute for Security Studies, 2017), 17, https://www.iss.europa.eu/sites/default/files/EUISSFiles/After_EU_Global_Strategy._Resilience.pdf.

6 Julian King, "Democracy Is under Threat from the Malicious Use of Technology. The EU Is Fighting Back," *The Guardian*, July 28, 2018, www.theguardian.com/commentisfree/2018/jul/28/democracy-threatened-malicious-technology-eu-fighting-back.

state capture by political elites, the rise of authoritarianism and populism,[7] that are and can be aggravated by direct interference from non-democratic foreign powers. This interference stems from the competition between democratic and authoritarian major international actors, a result of the shift towards a multipolar distribution of power in the global system.

Undermining trust and manipulation of public opinion were predominantly used in domestic politics by internal actors and just subsequently employed in the international relations power play.

Today, two major interrelated trends make imperative the assessment of how democratic institutions are undermined. Equally necessary and urgent is the implementation of measures to counter the threats and increase the resilience of democratic institutions and processes.

The first trend stands at the intertwining between technology, social, and political malicious actions. It is generally acknowledged that social media and the new electronic means of dissemination and the automation of messages enable communication at the speed of light. Although the internet has immense democratic potential, information and the technology for dissemination might be and often are *weaponized* for attaining political goals, mostly targeting the subversion of consolidated democracies. Such a political strategy that uses computational means is closely associated with the deliberate generation and use of misinformation, targeting political adversaries and the democratic processes and institutions as such, at a scale and magnitude unseen until now. (As early as 2014, the World Economic Forum identified the rapid online spread of misinformation as one of the top 10 perils to society[8]).

The second essential trend is the exponential *increase of foreign influence operations*, interfering in and undermining fundamental political processes from elections to a broad spectrum of "hybrid attacks" to undermine democracy. "Hybrid threats" are defined as coordinated and synchronized actions that deliberately target democratic states and institutional vulnerabilities through political, economic, military, civil, and information-related means.[9]

Foreign influence operations by autocratic powers, understood as manifestations of "sharp power,"[10] use extensively and in a concerted manner, *inter alia*,

---

[7] Timothy D. Sisk, "Democracy's Resilience in a Changing World," in *The Global State of Democracy: Exploring Democracy's Resilience* (Stockholm: International IDEA, 2017), 34-61, https://iknowpolitics.org/sites/default/files/idea-gsod-2017-report-en.pdf.

[8] World Economic Forum, "Top 10 Trends of 2014," in *Outlook on the Global Agenda 2014*, http://reports.weforum.org/outlook-14/top-ten-trends-category-page/10-the-rapid-spread-of-misinformation-online. For a detailed analysis see Wooley and Howard, eds., *Computational Propaganda*, 168.

[9] The European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE, "Hybrid Threats," https://www.hybridcoe.fi/hybrid-threats.

[10] Christopher Walker and Jessica Ludwig, "The Meaning of Sharp Power: How Authoritarian States Project Influence," *Foreign Affairs*, November 16, 2017, www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power. According to Walker and Ludwig: "Authoritarian influence efforts are 'sharp' in the sense that they pierce,

the above-mentioned technological tools. In this context, the actions sponsored by the Russian Federation represent the most concerning and well-documented cases of foreign influence operations.[11]

It is critical to understand how democratic processes and institutions can be attacked both by internal political actors and by foreign rivals and adversaries, by undermining the trust of people in democracy through political manipulation using the new communication technologies. For that, we need to make a short introduction to recent advances in information technology and the specifics of *computational propaganda*, an extremely powerful new communication tool used against democratic actors and institutions worldwide. Powerful and often anonymous political actors have used computational propaganda techniques to interfere in national elections, perpetrate political attacks, spread disinformation, censor and attack journalists, and create fake trends.

This analysis is performed from a *political science perspective*, yet it is clear that technical data should be presented to a broader audience outside the confined space of the specialists in information technology. Decision-makers and public opinion must be aware that "coordinated efforts are even now working to seed chaos in many political systems worldwide. Some militaries and intelligence agencies are making use of social media as conduits to undermine democratic processes and bring down democratic institutions altogether."[12] Specialists in computational propaganda warn that describing the phenomenon only from a technical standpoint (as a set of variables, models, codes, and algorithms) will create the delusion of propaganda being "unbiased and inevitable," and ask for complementing the technical description with social and political assessments, which will equally present the harmful and dubious intentions and actions of the actors that use the computational propaganda tool.

According to Wooley and Howard, "computational propaganda is a term that neatly encapsulates this recent phenomenon—and the emerging field of study—

penetrate, or perforate the political and information environments in the targeted countries. In the ruthless new competition that is under way between autocratic and democratic states, the repressive regimes' sharp power techniques should be seen as the tip of their dagger. These regimes are not necessarily seeking to 'win hearts and minds,' the common frame of reference for soft power efforts, but they are surely seeking to manipulate their target audiences by distorting the information that reaches them."

[11] As the US National Intelligence Council concludes in 2017, Russian efforts (to influence the 2016 US presidential election) represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations. See National Intelligence Council, "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution," January 6, 2017, www.dni.gov/files/documents/ICA_2017_01.pdf.

[12] Wooley and Howard, eds., *Computational Propaganda*, 3.

of digital misinformation and manipulation."[13] *Computational propaganda is in fact a political strategy that relies on computational enhancement.* Detailed research has shown that social media platforms are "vehicles for manipulative disinformation campaigns." "Computational propaganda, therefore, forms part of a suite of dubious political practices that includes digital astroturfing,[14] state-sponsored trolling,[15] and new forms of *online warfare* known as PsyOps or InfoOps wherein the end goal is to manipulate information online in order to change people's opinions and, ultimately, behavior." Automation, scalability, and anonymity are hallmarks of computational propaganda.[16] Data-driven techniques and tools like automation (bots – *automatic software built to mimic real, human users*) and algorithms (decision-making code) allow small groups of actors to megaphone highly specific, and sometimes abusive and false, information into mainstream online environments.[17]

The use of "Big Data"[18] for political campaigning and, often, manipulation of the electorate is another highly concerning challenge to the functioning of democracy. Specialized data analytics companies are gathering information on the

[13] Wooley and Howard, eds., *Computational Propaganda*, 4.

[14] *Astroturfing* is the process of seeking electoral victory or legislative relief for grievances by helping political actors find and mobilize a sympathetic public using the Internet. This campaign strategy can be used to create the image of public consensus where there is none, or to give a false impression of the popularity of a candidate or public policy idea – see Howard (2005), quoted in Wooley and Howard, eds., *Computational Propaganda*.

[15] Trolling is, according to the Urban Dictionary, "the deliberate act (by a Troll – noun or adjective) of making random unsolicited and/or controversial comments on various internet forums with the intent to provoke an emotional knee jerk reaction from unsuspecting readers to engage in a fight or argument." Tech Policy, "State-sponsored trolling is rampant throughout the world – including the US," *MIT Technology Review,* July 19, 2018*,* www.technologyreview.com/f/611694/state-sponsored-trolling-is-rampant-throughout-the-world-including-in-the-us/. State-sponsored trolling: "Using fake accounts, bots, and coordinated attacks by legions of followers, governments make it extremely difficult to distinguish between public opinion and sponsored trolls."

[16] Wooley and Howard, eds., *Computational Propaganda*, 7.

[17] According to Wooley and Howard, "The use of bots for malicious purposes, including undermining democratic institutions, is particularly concerning, as—according to recent data, bots generate almost half of all Web traffic—an extraordinary proportion," Wooley and Howard, eds., *Computational Propaganda*, 8

[18] The term is associated with the 2001 definition by the industry analyst Doug Laney who described the "3Vs": volume, variety, and velocity, as the key "data management challenges." According to the Oxford English Dictionary, big data is "data of a very large size, typically to the extent that its manipulation and management present significant logistical challenges." The data sets to be analyzed are too large or complex to be dealt with by traditional data-processing application software. Most relevant for the use of big data in digital campaigning were the use of predictive analytics, user behavior analytics, or certain other advanced data analytics methods that extract value from data.

identities, beliefs, and habits of the potential voters, who can be afterward targeted with specific messages designed to influence and change their political decisions.

The Facebook/Cambridge Analytica data scandal related to the Leave.EU campaign during the June 2016 referendum in Britain and the Trump election campaign generated the most intense parliamentary and public scrutiny as well as legal responses to the risks of using voters profiling and illegal gathering of their personal data. The profiles of 87 million Facebook users were hijacked to identify their subconscious biases and trigger anxieties for manipulating their political decisions. Analysts agree that it is difficult to evaluate the degree to which the use by the campaigns of the data sets created by Cambridge Analytica for micro-targeting—individualized political messaging—swayed the public opinion and changed the results of the 2016 votes in the UK and the US. The need for greater oversight over the use of social network platforms by political campaigns during the electoral process was recognized immediately and democratic governments are initiating legal and regulatory responses.

> *The weaponization of on-line fake news and disinformation poses a serious security threat to our societies. The subversion of trusted channels to peddle pernicious and divisive content requires a clear-eyed response based on increased transparency, traceability and accountability. Internet platforms have a vital role to play in countering the abuse of their infrastructure by hostile actors and in keeping their users, and society, safe.*
>
> EU Security Commissioner Julian King[19]

The European Commission's *Communication on Tackling Online Disinformation*[20] defines disinformation as "verifiably false or misleading information that is created, presented and disseminated for economic gain or to deceive the public intentionally, and in any event to cause public harm." It clarifies that this definition excludes reporting errors, satire and parody, partisan news and commentary, or illegal content. It distinguishes between verifiably false news and misleading information.

Trust in democratic institutions can also be undermined by *political campaigns* based on false/fake news distributed through more traditional mass media as well as widely by social media platforms. This is particularly concerning as,

---

[19] EU Commission, "Tackling Online Disinformation: Commission Proposes an EU-wide Code of Practice," April 26, 2018, https://europa.eu/rapid/press-release_IP-18-3370_en.htm.

[20] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Tackling Online Disinformation: A European Approach, Shaping Europe's Digital Future, Brussels, April 26, 2018, https://ec.europa.eu/digital-single-market/en/news/communication-tackling-online-disinformation-european-approach.

until recently, political representation was mainly done through elected representatives, like the members of parliament, and now citizens are expressing themselves directly, being more vulnerable to these campaigns.

Our understanding of present-day threats and vulnerabilities to democratic political systems needs to consider the damaging use of fake, sensational, and other forms of "junk news" during sensitive political moments over the last several years. O'Connor synthesizes the phenomenon accurately: "We live in an age of misinformation – an age of spin, marketing, and downright lies. Of course, lying is hardly new, but the deliberate propagation of false or misleading information has exploded in the past century, driven both by new technologies for disseminating information—radio, television, the internet—and by the increased sophistication of those who would mislead us."[21]

The main goal of the disinformation campaigns is to create an emotional decision-making environment to replace reason and factual-based judgment as a working method.

Furthermore, the current intellectual debate on the "post-truth society" reveals that some political strategists are openly embracing challenging truth itself "as a strategy for the political subordination of reality." "Thus, what is striking about the idea of post-truth is not just that truth is being challenged, but that it is being challenged as a mechanism for asserting political dominance."[22] We risk ending up in parallel realities, being difficult to distinguish which one is true.

A relevant case study for foreign influence operations is the increasingly well-documented attempts by Russia to "undermine unity, destabilise democracies and erode trust in democratic institutions. This pattern has been repeated in the EU: from the influence operations in the run-up to the 2016 referendum in the Netherlands about the EU-Ukraine Association Agreement; continued cyber-attacks to further reduce trust in the wake of the UK EU membership vote; Kremlin-affiliated media promotion of polarising issues during the 2017 German election; and pro-Kremlin bots engaging in a coordinated 'disruption strategy' over Catalonia in 2017, along with Kremlin-backed news platforms."[23] In the *Report on the Investigation into Russian Interference in the 2016 Presidential Election,* Special Counsel Robert S. Mueller concluded that "The Russian government interfered in the 2016 presidential election in a sweeping and systematic fashion."[24]

---

[21] Cailin O'Connor and James Owen Weatherall, *The Misinformation Age: How False Beliefs Spread* (New Haven, CT: Yale University Press, 2019), 11.

[22] Lee McIntyre, *Post-Truth* (Cambridge, MA: MIT Press, 2018), Chapter 1, Kindle Edition.

[23] Naja Bentzen, "Foreign Influence Operations in the EU," *European Parliamentary Research Service Briefing*, July 2018, http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625123/EPRS_BRI(2018)625123_EN.pdf.

[24] U.S. Department of Justice, Special Counsel Robert S. Mueller, III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, Volume 1 (Washington, D.C., March 2019), https://cdn.cnn.com/cnn/2019/images/04/18/mueller-report-searchable.pdf.

According to the European Parliament *Resolution on EU strategic communication to counteract propaganda against it by third parties:* "Russian strategic communication is part of a larger subversive campaign to weaken EU cooperation and the sovereignty, political independence and territorial integrity of the Union and its Member States." The European Parliament "urges Member State governments to be vigilant towards Russian information operations on European soil and to increase capacity sharing and counterintelligence efforts aimed at countering such operations."[25]

The spectrum of threats and undermining actions to democratic institutions and processes is broader than briefly introduced in the paper. There is increasing consensus both at national and inter-governmental level that *increasing democratic resilience* can prepare better responses to shocks and stresses, including those generated and disseminated via computational means.

The *notion of 'resilience'* is extensively used in different domains from biology and ecology to disaster response, development, humanitarian aid, democracy, foreign policy, society as a whole, critical infrastructures, cyber, etc. Therefore, in the last two decades, the notion was perceived by most analysts as a 'buzzword' that maintains, nevertheless, its practical utility when applied to a context-specific framework.

In the simplest definition, resilience refers to *the capacity to absorb and recover from any type of stress or shock*. Definitions become more complex yet not always more convincing when the term is associated with a specific system or goal to be attained. Without entering the debate on the usefulness or otherwise of the term, we can agree with Rhinard[26] that any specific approach needs to clarify the following five central questions: (1) *what is resilience?*, respectively the value of a broad and expansive or of a narrow definition; (2) *who (or what) should be resilient?,* meaning the priorities set by different academic disciplines for the resilient individual, community, state or society as a whole; (3) *when can we expect resilience to happen?*, i.e., resilience can be understood either as a "bounce-back" capacity taking place after an extreme event has hit or as "anticipatory resilience" taking place before a disturbance actually occurs and, in the best scenario, even preventing it from happening; (4) *what kinds of events do we hope to be resilient against?* – crises that are outside the realm of imaginable ("black swans"[27]) or focus on "normal emergencies," where resilient systems absorb and adapt to these problems and prevent them from becoming even worse;

[25] European Parliament, "EU Strategic Communication to Counteract Anti-EU Propaganda by Third Parties, European Parliament Resolution of 23 November 2016 on EU Strategic Communication to Counteract Propaganda against It by Third Parties (2016/2030(INI))," www.europarl.europa.eu/doceo/document/TA-8-2016-0441_EN.pdf.

[26] Mark Rhinard, "Horizontal Issues," in *After the EU Global Strategy*, 25-27.

[27] Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable*, 2nd ed, (New York: Random House, 2010).

and finally (5) *can resilience be engineered?*, focusing on the effectiveness of designed public policies for building resilience.[28]

The International Institute for Democracy and Electoral Assistance explores solutions for building *democratic resilience*: the ability of democratic ideals, institutions, and processes to survive and prosper when confronted with challenges and the crises they may produce.[29]

In IDEA's definition, "resilience refers to properties of a political system to cope, survive and recover from complex challenges and crises that represent stresses or pressures that can lead to a systemic failure."[30] According to Sisk, "chief among the *properties of resilient social systems* are: 1) *Flexibility*: the ability to absorb stress or pressure; 2) *Recovery*: the ability to overcome challenges or crises; 3) *Adaptation*: the ability to change in response to a stress to the system; and 4) *Innovation*: the ability to change in a way that more efficiently or effectively addresses the challenge or crisis."[31]

Fostering state and societal resilience as well as the resilience of democratic institutions and processes are interrelated and should be designed in a coordinated manner. This is also true for policies that respond to specific, sub-system level problems, thus ensuring the resilience of critical infrastructures, respectively cyber-, energy- or climate-change resilience, just some examples, should be coordinated and integrated into the overall efforts of increasing state and societal resilience.[32] Analysts consider that democracy can enhance and contribute to the community, societal, and state resilience. Democratic systems are, under certain conditions, more flexible and able to adapt to change and embrace innovation. It is, therefore, of critical importance that democratic resilience is ensured and enhanced.

Resilience building must be context-specific as there are no one-size-fits-all solutions for approaching different challenges, vulnerabilities, and threats and reinforcing the capability of social systems to absorb and recover from any kind of stress and shock.

Thus, it is necessary to have specific resilience-building measures to respond to each of the challenges that undermine democratic institutions and processes.

---

[28] Rhinard, "Horizontal Issues," 27.

[29] Sisk, "Democracy's Resilience in a Changing World."

[30] Timothy D. Sisk, "Democracy and Resilience: Conceptual Approaches and Considerations," Background Paper (Stockholm: International Institute for Democracy and Electoral Assistance, 2017), 5, https://www.idea.int/gsod-2017/files/IDEA-GSOD-2017-BACKGROUND-PAPER-RESILIENCE.pdf.

[31] Sisk, *Democracy and Resilience*, 5.

[32] Some authors consider resilience a form of *governamentality*. According to Joseph, resilience, despite its claims to be about the operation of systems, is, in practice, closer to a form of governance that emphasizes individual responsibility. Nevertheless, if building resilience is understood simply as good governance, the usefulness of the term is doubtful. See Jonathan Joseph, "Resilience as Embedded Neoliberalism: A Governmentality Approach," *Resilience: International Policies, Practices and Discourses* 1, no. 1 (2013), 38-52, https://doi.org/10.1080/21693293.2013.765741.

Policies to increase democratic participation, respond to disinformation campaigns, counter hybrid threats, enhance cyber and infrastructure resilience, etc., need to be coordinated at national and intergovernmental levels. The EU and NATO are developing and implementing complex resilience-building measures at the level of their member states, as well as in close EU-NATO cooperation, boosted by strengthening the strategic partnership as defined by the two Joint Declarations approved in Warsaw in June 2016 and Brussels in May 2018.[33]

Building resilience is *a core element of the collective defense* of the North Atlantic Alliance.[34] Strengthening state and societal resilience is key to the EU approach to the security of the Member states and the Union, particularly for the relations with the partners in the South and the East, as presented in the EU's Global Strategy for Foreign and Security Policy.[35] The EU has adopted *key documents on resilience*, including on countering disinformation.[36] A very relevant initiative, in this context, is the self-regulatory Code of Practice on Disinformation

[33] "Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of NATO," Warsaw, July 8, 2016, https://www.consilium.europa.eu/media/24293/signed-copy-nato-eu-declaration-8-july-en.pdf; and "Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization," Brussels, July 10, 2018, www.nato.int/cps/en/natohq/official_texts_156626.htm.

[34] NATO official text, "Commitment to Enhance Resilience Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw, 8-9 July 2016," https://www.nato.int/cps/en/natohq/official_texts_133180.htm. For an analysis see: Jamie Shea, "Resilience: A Core Element of Collective Defence," *NATO Review*, March 30, 2016, https://www.nato.int/docu/review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm. A relevant perspective on NATO's national resilience obligations in Madeleine Moon, "NATO's National Resilience Obligations," *RUSI Commentary*, March 15, 2019, https://www.rusi.org/commentary/NATOs-National-Resilience-Obligations.

[35] "The EU will foster the resilience of its democracies, and live up to the values that have inspired its creation and development. These include respect for and promotion of human rights, fundamental freedoms and the rule of law. They encompass justice, solidarity, equality, non-discrimination, pluralism, and respect for diversity. Living up consistently to our values internally will determine our external credibility and influence." "Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy," June 2016, 15, and "State and Societal Resilience to Our East and South," 23-28, https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf.

[36] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication to the European Parliament and the Council. A Strategic Approach to Resilience in the EU's External Action," June 7, 2017, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52017JC0021; European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Tackling Online Disinformation: A European Approach," Brussels, April 26, 2018, https://ec.europa.eu/digital-single-market/en/news/communication-tackling-online-disinformation-european-approach.

agreed in September 2018 by representatives of online platforms, leading social networks, and the advertising industry agreed to address the spread of online disinformation and fake news.[37]

A significant number of commonly agreed actions, implemented jointly by EU and NATO, focus on resilience building, particularly on countering hybrid threats, analysis, and coordinated strategic communication to spot disinformation and communicate a credible narrative, cyber defense, etc.[38] It is also worth mentioning the activity of the NATO STRATCOM Centre of Excellence and of the European Centre of Excellence for Countering Hybrid Threats functioning as a neutral facilitator between the EU and NATO through strategic discussions and exercises.[39]

International organizations—both intergovernmental and non-governmental like the OECD, various UN agencies, and IDEA International—have proposed specific frameworks for building and strengthening the state, societal and democratic resilience. A comparative analysis of these initiatives at the level of democratic states, EU and NATO, and other international organizations, as well as of the public-private initiatives for implementing specific resilience policies, goes well beyond the scope of this article.

A certain number of *measures to restore trust in democratic institutions*, counter disinformation and fake news, and act against computational propaganda are nevertheless worth mentioning. In essence, there is a need for basic, solid political education for the citizens and the electorate, as well as actions to counter foreign interference and specific measures of surveillance up to the vote. "The life-long development of critical and digital competences, in particular for young people, is crucial to reinforce the resilience of our societies to disinformation."[40] The measures proposed by the US National Democratic Institute can offer good practices for countering disinformation in politics, particularly elections, respectively by conducting research on disinformation vulnerability and resilience; monitoring disinformation and computational propaganda in elections; strengthening political party commitments to information integrity; helping social media platforms and tech firms "design for democracy"; sharing tools to detect and disrupt disinformation and rebuilding trust in institutions and processes through democratic innovation.[41]

The advance of democracy at a global scale has had its ebbs and flows in recent history and we believe that the democratic form of government will prove its attractiveness and resilience in spite of current serious challenges. In the end,

---

[37] European Commission, "Code of Practice on Disinformation," September 26, 2018, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

[38] EEAS, "EU-NATO Cooperation – Factsheets," June 17, 2020, https://eeas.europa.eu/headquarters/headquarters-homepage/28286/eu-nato-cooperation-factsheet_en.

[39] European Centre of Excellence for Countering Hybrid Threats, "Functions of Hybrid CoE," https://www.hybridcoe.fi/.

[40] European Commission, "Tackling Online Disinformation."

[41] National Democratic Institute, "Info/tegrity. An NDI Initiative to Protect the Integrity of Political Information," https://www.ndi.org/infotegrity.

it is a new and elevated form of the age-old battle for winning minds and hearts. Established democracies are more and more aware of the new challenges and started substantive legal and regulatory work on enhancing the resilience of democratic institutions and processes. The challenges and threats presented in the article indicate a long-term trend with evolutions that are difficult to predict. The legal and regulatory response frameworks will need to be coordinated and continuously adapted to the rapidly changing threat environment.

Disclaimer

The views expressed are solely those of the authors and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

Acknowledgment

Connections: The Quarterly Journal, Vol. 19, 2020 is supported by the United States government.

About the Author

Dr. **Ioan Mircea Paşcu** is Professor of International Relations, National School of Political and Administrative Studies (since 1990). He was Vice-President of the European Parliament (November 2014 – July 2019), Vice Chair of the Committee on Foreign Affairs, European Parliament (2007-2017). He was Minister of Defense of Romania (2000-2004), contributing substantially to the admission of Romania into NATO. Presidential counselor, Head of Foreign Policy Department of the Romanian Presidential Administration (1990-1992), Vice-President of the National Salvation Front (1990-1992), State Secretary, Deputy Minister of Defense (1993-1996), Chairman of the Committee on Defense, Public Order and National Security, Chamber of Deputies of the Romanian Parliament (1996-2000), Member of the Romanian Parliament (1996-2007), Vice-President of the Social Democratic Party (1997-2006). Dean of the Faculty of International Relations, National School of Political and Administrative Studies (1990-1996). Chair of International Relations, National School of Political and Administrative Studies (2004-2009). E-mail: puiu.pascu@gmail.com

Dr. **Nicolae-Sergiu Vintila** is currently working as a policy analyst at the European Parliamentary Research Service of the European Parliament. He has been a policy advisor to Prof. Ioan Mircea Pascu MEP, Vice-President of the European Parliament, between 2009-2019. Between 2001 and 2009, he held senior management positions in the Ministry of Defense of Romania. Dr. Vintila was a researcher at the Romanian Academy (1990-1997), and since 1990 he is a lecturer and associate professor in International Relations and taught courses primarily for postgraduate students at the National School of Political Studies and Public Administration in Bucharest and the University of Luxembourg. He writes in his own capacity. E-mail: nicolae-sergiu.vintila@ext.uni.lu