Research Article **Open Access**

Shota Gvineria*

Euro-Atlantic security before and after COVID-19

https://doi.org/10.2478/jobs-2020-0005
received June 19, 2020; accepted June 24, 2020.

Abstract: Contemporary global power competition has turned the world into a hybrid battlefield. In modern battlefield, authoritarian regimes have the strategic advantage of being irresponsible, reckless and aggressive. This advantage is combined with the ability of the authoritarian regimes to find cheap and effective - short of war - solutions for achieving geopolitical objectives. In past decades authoritarian regimes such as Russia and China have been actively applying hybrid strategies against the Western dominated rules based international system. Those strategies are being constructed based on identification and utilization of the vulnerabilities of the democratic political systems, institutions and societies. Pandemic crisis caused by unpredictable and unprecedented spread of the mutated new Corona virus, have underlined vulnerabilities and opened up new possibilities for the hybrid warfare. The pandemic influences every power on the global stage, but will COVID-19 be a turning point for the Euro-Atlantic Security environment?

Keywords: Hybrid warfare; COVID-19; Security environment; Euro-Atlantic Security; Cybersecurity; Information warfare.

1 Hybrid threats to Euro-Atlantic security before and after COVID-19: a game-changer virus?

At the beginning of the 20th century, an Italian philosopher, Antonio Gramsci, wrote the lines that perfectly described the existing state of affairs in his times – 'old world is dying, and the new world struggles to be born: now is the time of monsters'. Perhaps, this quote applies to the 21st century even more. During the past decade, politicians and experts have repeatedly stated that the security environment is experiencing unprecedented pressure due to the complexity of modern threats and challenges. For many commentators, Gramsci's ideological monsters have evolved into populist, extremist and ultranationalist movements complementing the hybrid warfare toolkits of the authoritarian and revisionist[1] regimes. For others, climate change and the devastating human influence on the environment are seen as the imminent contemporary threats. However, the most underrated monster of modern times appears to be a mutated new coronavirus or corona virus disease 2019 (COVID-19) – arguably the greatest security shock and game changer since 11 September 2001 terrorist attack on the US.

The outbreak of the pandemic and its shocking effects have underlined the unpredictable and uncertain nature of the contemporary security environment. Total panic, unprecedented human lockdown and apocalyptic interruption of global interaction even raised associations with World War III among some commentators (Hormats, 2020). Unlike Nuclear War or Cyberwar, anticipated in not only science fiction but also many academic works through previous decades, the world is now fighting a war against an invisible enemy. Still, some sceptics think that the expected impact of the pandemic is exaggerated (RFI/AFP, 2020). The lack of information about the genesis and features of the virus has fuelled panic and contributed to the contamination of the information environment. While everyone's crystal ball

1 The term 'revisionist' is defined in the following page. Meanwhile, this article suggests that while all revisionist powers are authoritarian, not all the authoritarian regimes are revisionist

***Corresponding author: Shota Gvineria,** Baltic Defence College, Estonia, E-mail: shota.gvineria@baltdefcol.org

is broken and a comprehensive solution to the crisis is nowhere in sight, it will probably take months, if not years, to evaluate and analyse the consequences of the COVID-19 crisis.

However, despite global confusion, some determinants of the modern security environment can still be identified and studied. Therefore, the article attempts to outline some key variables that form the security paradigm in the Euro-Atlantic area. The focus is to identify the key vulnerabilities of the Euro-Atlantic community, which are exploited by Russia and China for the effective application of their hybrid warfare toolkits. In the first part, the article defines hybrid warfare and its role in the formation of the security environment in the Euro-Atlantic area before the outbreak of COVID-19. The second part of the study focuses on the expected impact of the pandemic crisis on Euro-Atlantic security in the context of hybrid warfare. Both parts specifically focus on cyberspace and the information ecosystem, which are defined by the study as indispensable and the most important elements for waging hybrid warfare. Since hybrid warfare includes utilisation of all elements of national power, the heavy concentration on cyberspace and informational aspects as enablers, as well as tools of hybrid warfare, is an important limitation of the research.

The primary challenge during the research has been the constantly evolving COVID-19 situation at the moment of writing. Another challenge relates to the scope of the research, as there is already overwhelming material defining and describing hybrid warfare. Still, the ambition of the study is to provide a clear and pragmatic definition of hybrid warfare and practically link its theoretical part with the developments in Euro-Atlantic security on the ground. To take advantage of the existing extensive data, secondary data analysis of available literature and synthesis of findings from multiple studies have been utilised for describing the hybrid warfare trends before the pandemic. For the second part of the research, since very little scientific literature is available on the ongoing pandemic crisis, the primary source of the data obtained comes from the op-eds of influential opinion makers and news articles. Thus, a mixed methodology is used in the study, which contains both qualitative and quantitative elements.[2]

Another source, which adds significantly to the qualitative research and also covers the quantitative part, is the survey specifically designed to study the perceptions of subject matter experts. Eight questions included in the survey are aimed at collecting projections made by the experts on the anticipated effect of the pandemic crisis on Euro-Atlantic security architecture in general and its impact on key aspects of hybrid warfare in particular. The questions contain multiple-choice options as well as sections for general comments. Eighteen subject matter experts were selected for the survey based on their diverse research interests and different perspectives on Euro-Atlantic security. An essential selection criterion was geographical coverage, which was focussed on reflecting the diversity of opinions from North America to Russia and from Western and Northern Europe to the Baltic and Black sea regions. The survey was conducted during the evolving crisis, in the period of 6–24 May 2020. The combination of various sources and types of data attempts to address the challenging aspects of the study more comprehensively.

2 Hybrid threats before the pandemic: a world with blurred boundaries

From a broader perspective, the greatest challenge to Euro-Atlantic security in recent decades has been the rise of authoritarian regimes and their aggressive policies against the Western-dominated rules-based, liberal world order.[3] The term ‘revisionism’ has been actively used among foreign policy experts to describe the process of undermining of the liberal principles and frameworks of global interaction, as well as the authoritarian policies undermining democratic values and institutions (Pisciottta, 2020). Russia and China have been aggressively applying various tools of hybrid warfare for the implementation of revisionist policies to oppose Western interests and values not only in their respective neighbourhoods but also globally. A creature from Greek mythology – Centaur – is a good analogy to explain hybridity. From different perspectives, Centaur could be equally seen as a man or as a horse; however, it is neither a man nor a horse. Centaur is a hybrid creature combining elements of both. Similarly, hybrid warfare combins the elements of the hard as well as soft power.

2 This research was supported by a Marie Curie Research and Innovation Staff Exchange scheme within the H2020 Programme (grant acronym: New Markets, no. 824027).

3 For the definition of the liberal world order, please see: https://medium.com/@jackkrupansky/elements-of-the-liberal-world-order-d6e1a83813dd.

For this article, hybrid warfare will be defined as a coherent strategy of applying all elements of national power interchangeably or simultaneously with the aim of identifying vulnerabilities of the adversary and turning them into pressure points. It is very important to note that a coherent strategy does not mean that all instances of hybrid warfare are interconnected and synchronised on the operational level. Rather, coherent strategy accentuates the continuity of the process whereby adversaries are constantly trying to exploit vulnerabilities and attempt to use the weaknesses of one another. Simply put, hybrid warfare strategies depend on the opportunities that arise so as to advance predetermined overarching objectives. Hybrid warfare may look chaotic because those random opportunities guide specific operations in different points in time. Thus, coherent hybrid warfare strategy implies careful calculation of which tools would be more productive, relevant and efficient based on the context in which particular operations take place. This key feature makes hybrid warfare coherent, complex and chaotic – all at the same time. Its indefinite continuity and opportunity-based application are the primary reasons why hybrid warfare is so difficult to predict, counter or deter.

Although Russia and China share the overarching revisionist objectives, in most of the cases, they use different hybrid toolkits to achieve their specific operational goals in the Euro-Atlantic theatre. China's exceptional economic growth has facilitated its dominant role in East Asia; however, on the global stage, the main revisionist objective of challenging the US as a superpower remains to be achieved (Li & Shaw, 2014, p. 74). Meanwhile, with no remarkable financial resources and the deteriorating socioeconomic situation at home, Russia has had to rely on a combination of kinetic, political and information tools to maintain its domination through occupation and annexation in the neighbourhood (Aris & Tkachev, 2019). The same toolkit has been applied for maintaining Russian influence in the Middle East through military intervention in Syria, which in turn is an indirect claim of a world power status. Thus, while China relies more on the economic and financial tools of warfare, Russia is much more aggressively utilising a combination of overt and covert coercive means.

The West's lack of a unified strategy and a shared vision on countering – or even defining – critical threats and challenges has become an exploitable strategic vulnerability. There are vast variations on how security risks are prioritised even within the European and Euro-Atlantic institutions. For example, the countries bordering the Russian Federation in the so-called Eastern flank see Russia's aggressive policies as an existential threat. In contrast, among the countries of Western and Southern Europe, there is more focus on cooperation opportunities with Russia, while threats are often seen as exaggerated. Even when the threat is duly acknowledged, especially after the annexation of Crimea, the urgency of action to counter the shared threats is often discounted and prioritised differently according to the fractured East–West or North–South sub-regional viewpoints. These divides often contribute to the ambiguity and to the delayed consensual decision-making. The unified vision, and even more so – collective action, is seriously undermined by complicated global and geopolitical agendas, such as difficult transatlantic relations, disagreements within the European Union (EU) and Brexit. Accordingly, revisionist strategies often dwell on seeking to amplify divisions between governments and among societies.

In other words, the key defining factor of the pre-COVID-19 Euro-Atlantic security environment has been that both revisionists, Russia and China, have been trying to compete with the West to claim equal status as global powers by applying hybrid warfare strategies in different parts of the world. More specifically, China has been buying its influence by gaining access to strategic Western assets and infrastructure, while Russia has chosen disruptive active measures[4] and proxy warfare. The confusion caused by the complexity of countering a wide array of underlying modern security threats has defined the security environment in the 21st century. Although hybrid strategies and tools have been part of warfare for ages, the features of the modern globalised world have opened new possibilities for their application and have multiplied their far-reaching effects. It is evident that authoritarian regimes, encouraged by cautious or ambivalent Western strategies of countering hybrid threats, have turned their ability to escalate into a strategic advantage. A critical vulnerability facilitating revisionist objectives has been the political cohesion of Western countries, institutions and societies.

One of the critical characteristics of the globalised world, affecting the formation of the modern security environment the most, is the interdependence and connectivity between major powers in vital areas, such as production and supply chains, transport and communications infrastructure, and technology. The September 2001 (9/11) terrorist attacks on the US were a reminder that no single power can achieve security in isolation, by heavily relying on military force and by protecting the homeland only within its boundaries. In the aftermath of 9/11, understanding of national security has

4 The term 'active measures' in Russian: активные мероприятия - aktivnye meropriyatiya.

evolved into a broader phenomenon. It has become evident for the world powers that the sources of insecurity could easily reach the mainland of even the best-protected military superpowers from across very long distances in a short amount of time. Interconnectedness undermines geography and time as defining factors, and the physical as well as political boundaries have begun to fade away.

2.1 Boundaries between war and peace – unpeace

Authoritarian regimes have realised that the world of faded boundaries present wide possibilities for achieving revisionist ends. As the commander of Russian armed forces, General Gerasimov famously informed the world, 'today the boundaries between war and peace are blurred', meaning that hybrid warfare presents enormous opportunities to push a destructive agenda, but still stay below the threshold of conflict. Following the so-called Gerasimov doctrine, which is oriented at using information warfare and related subversion tools for disrupting democracy inside Western capitals, Russia has realised that one of the best ways to amplify the process of undermining democracy is to support peer authoritarian regimes. Russia's national hero, Colonel General Alexandr Dvornikov, had a chance to test his own hybrid warfare doctrine 2.0 while leading a military intervention in Syria in 2015. The doctrine relies on the deployment of 'integrated groups' of non-uniformed mercenary fighters, local regime-supported militias and regular troops to support regimes loyal to the Kremlin in different parts of the world (Tucker, 2019). The most recent demonstration of adopting the Dvornikov doctrine took place in Venezuela on a smaller scale, when Russia sent military personnel and equipment to support Maduro's regime (Reuters/Interfax, 2019). The doctrine also perfectly fits into the broader vision of President Putin's former ideological mastermind, Vladislav Surkov, namely that of extending Russia's political influence (Surkov, 2019). Surkov, in his monumental article 'Putin's lasting state', has clearly underlined the export potential of Russia's authoritarian political model as one of the powerful instruments of subversion.

On the one hand, Russia and China have adapted to the new realities and learned to take advantage of the vulnerabilities of the interconnected world through hybrid strategies. On the other hand, they are still going against the tide and are trying to bring back physical boundaries, division lines and spheres of influence. As part of the campaign to dominate the Western Pacific, China actively challenges freedom of navigation, including by building artificial island fortresses in its recently claimed international waters (Mandelbaum, 2019). In the case of Russia, Kremlin has demonstrated its willingness and ability to invade and occupy a neighbour's territory to reduce the likelihood of those countries escaping its 'sphere of exclusive influence'. Russia's resolve is evidenced by the launching of its military aggression against Georgia in 2008, followed by the annexation of Crimea and invasion of eastern Ukraine in 2014. Occupation, destabilisation and proxy warfare have become effective hybrid warfare tools for achieving revisionist goals.

To achieve political objectives in times of war or peace, an increasing number of states, as well as their proxies, continuously apply all possible tools at hand. As a result of the constant application of various hybrid tools, not only the regional security around China and Russia, but more broadly, the Euro-Atlantic security as a whole, is challenged. Military leaders, such as Gerasimov and Dvornikov, have started to develop evolving strategies, which adapt to new realities, by realising that there are more and more non-kinetic tools that can supplement, reinforce or even substitute military power. There is no declared beginning or negotiated end to hybrid warfare. In times of unpeace – a situation that is described as lack of peace but not necessarily a war – even the strongest and best-protected countries appeared to be inherently insecure (Merriam-Webster, 2020). Constant conflict has become the main feature of the contemporary security environment in the Euro-Atlantic area and beyond.

2.2 Boundaries between cyber and real environments

The security environment is an ever-evolving phenomenon and always follows in the footsteps of the changes on the planet. In the Clausewitzian world, there two military domains – land and sea. As a result of the breakthrough in aviation engineering, the World War I marked the emergence of the air as one of the key military domains. Alongside the technological breakthrough during the cold war period, space became another domain for the rivalry between adversaries. Today, when dependency of the world powers on the internet, as well as reliance on technological

solutions, is growing day by day, the kinetic possibilities of the cyber domain become more apparent. Thus, with hybrid warfare and constant conflict as a new normal, the boundaries between what is cyber and what is real are becoming increasingly blurred.

Cyberspace is largely mystified and considered to be an area of uncertainty. A commonly agreed understanding, however, is that cyberspace is the key instrument of hybrid warfare, as well as the defining factor of the modern security environment. As a human-made environment, cyberspace is a technology itself, which is used to exploit and to navigate all other domains - land, sea, air and space. Therefore, cyberspace has also changed the ways of using all instruments of national power and thus has evolved into the key enabler of hybrid warfare. On the other hand, far-reaching kinetic consequences of cyber effects can also be seen as one of the most powerful tools of hybrid warfare. Moreover, the US national strategy to secure cyberspace, from 2009 onwards, expressively regards cyberspace as the 'nervous system of the country' due to the vital role of protecting critical infrastructure for ensuring national security in the digital era (CISA, 2009). More specifically, in the modern world, essential services such as healthcare, transportation, telecommunications, banking, quality of food and many other vital processes, which have a direct impact on the normal functioning of the state, are either happening in cyberspace or heavily rely on internet connection. These are a few reasons why the cyber domain gives revisionist regimes an exceptional opportunity for pushing their disruptive agendas by operating below the threshold of conflict.

Growing numbers of malign actors are continuously trying to take advantage of inherent vulnerabilities and 'weaponise' cyberspace. In addition to the operational problems of cybersecurity, there are policy dilemmas that render ensuring stability in cyberspace a strategic challenge. There is even no universal definition of responsible behaviour in cyberspace. Despite attempts within the UN framework, there is still no agreed code of conduct to ensure that normative considerations can deter malicious activities.[5] Most importantly, there are no enforcement mechanisms to impose consequences for the malign activities in cyberspace. There has been some progress in synchronising cyber policies at least within the EU and the North Atlantic Treaty Organization (NATO) formats. However, Western powers are still divided on defining the proportionality of joint response to cyberattacks and on the criteria of attributing attacks to the aggressor. The lack of clarity on key policy considerations emboldens Russia and China to utilise cyberspace to encourage the proliferation of violence and challenge democratic values (Paterson & Hanley, 2020). With growing digitalisation of the vital processes in democratic countries, and with more reliance on technological solutions such as artificial intelligence and machine learning, cyberspace has emerged as a perfect domain for cyber-enabled influence operations.

China has been primarily using cyberspace to enable economic tools of hybrid warfare and cyber espionage to advance its economic interests through efforts to steal intellectual property and commercial secrets from the world's biggest technology service providers (Stubbs et al., 2019). Despite official denials by the Chinese government, high-complexity cyberattacks have been attributed to groups affiliated with official Beijing, such as Cloud Hopper. This group acquired its name for following business chief executive officers (CEOs) across international borders hopping from one breached network to another in different countries. Russia has been utilising cyberspace to achieve political gains, mainly through discrediting and compromising adversaries. The most symptomatic use of Russia's cyber capabilities is reflected in multiple reports on Kremlin's interference attempts into the electoral processes of democratic countries, such as the US, France and Germany (Goldman et al., 2020). Moreover, in 2019, the UK's National Cyber Security Centre (NCSC) directly accused the Russian military intelligence (GRU) of carrying out a large-scale cyberattack against Georgia's sovereignty by defacing many governmental and media web pages (FCO, 2020). Russian hacker organisations such as 'Fancy Bear' are reportedly carrying out cyberattacks authorised by Russian special services (NCSC, 2018).

There is a core difference between the cyber footprints of China and Russia due to the asymmetry of capabilities. Chinese company Huawei, which denies any collusion with official Beijing, has been caught for leaving so-called 'backdoors' in their equipment. The backdoors allow hackers who are aware of the vulnerability to compromise users in several different ways. Huawei corrected the flaw quickly after it was publicised; however, there are some doubts whether the gap was an unintentional software engineering mistake. Still, Huawei is playing an essential role in developing future technologies such as 5G, which in turn will be critical for further developments in the fields of artificial intelligence and machine learning (Wakefield, 2019). There have been similar security concerns related to the Russian smaller-scale software developer Kaspersky, which also denies ties with the Kremlin. The company has left

5 For UN cybersecurity working formats, please see: https://dig.watch/processes/un-gge.

similar backdoors, which has allowed unauthorised monitoring of its customers' online activities (Su, 2019). While China produces significant cyber capabilities, including hardware and software, Russia's achievements are limited. However, Russia's blatant and coercive manipulation within cyberspace leaves an exaggerated impression regarding Russia as a cyber superpower.

Another essential aspect of cyberspace in the context of hybrid warfare is its rapidly growing role in the military. In addition to being a military domain in itself, cyberspace has evolved into a force enabler and multiplier of warfighting capabilities. According to the policies and doctrines of many modern armed forces such as the US and France, cyber power is the ability to achieve and maintain superiority in the cyberspace domain to influence adversary behaviour, deliver strategic and operational advantage for the military force, and defend and advance national interests. China's military cyber capabilities have been fully integrated into its overall military strategy. China's cyber considerations evolve holistically in correlation with its understanding of the national security environment, domestic situation and activities of foreign militaries (Jinghua, 2019). Russia has demonstrated its cyber warfare capabilities by synchronising its military operations with cyberattacks as early as in 2008, during its invasion of Georgia. It is almost impossible to trace cyberattacks to specific actors based on hard evidence with full certainty. Revisionist powers understand that retribution in cyberspace requires political resolve, which makes attribution mostly a strategic choice rather than a technical issue. Thus, by taking advantage of cyber policy dilemmas and recognising that deterrence in cyber domain is more complicated than in other military domains, Russia and China increasingly rely on cyberspace military operations.

Finally, cyberspace is an information-based domain, which is perhaps its most important feature, as information has clearly become a vital resource and source of power in the era of hybrid warfare. Cyberspace has fundamentally changed the paradigm of navigating the information environment. First, the internet has enabled full digitalisation of the ways to create, store, modify, exchange and exploit information. Digitalisation of the information, in turn, has accumulated an overwhelming amount of information and data openly available on the internet. As of May 2020, almost 1.8 billion websites are available online, and approximately 8 billion gigabytes of online traffic is generated daily (Internet Live Stats, 2020). Such a complex information ecosystem has boosted the importance of the informational aspect of cybersecurity. The challenge of information security in modern times implies ensuring all aspects of the so-called CIA triad – confidentiality, integrity and availability – simultaneously and continuously. From the operational perspective, this means 24/7 defence of systems and networks from unauthorised access and unauthorised modification of information while preventing adversaries from interruption of one's own access to information. Overwhelming amounts of online information have shifted the objectives of information consumption for the people or the users. If, in the pre-internet era, information consumers were striving to find channels and get access to information, now, the objective is to determine the credibility of the information. High levels of confusion and uncertainty offered by the modern information environment, in combination with the vulnerabilities of cyberspace, provide vast opportunities for waging information warfare.

2.3 Boundaries between the truth and falsity

The contemporary information environment, in which the boundaries between the truth and falsity are blurred, sets the most favourable context for the revisionist offensive against democracy in the post-fact or post-truth era. In 2016, the Oxford Dictionary defined 'post-truth' as 'Relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief' (Wang, 2016). This new reality fundamentally transformed the information ecosystem. It empowered the most disturbing modern trends, such as increasing dismissal of not only science but also evidence, facts and even truth itself (McIntyre, 2018). In practice, this translates into the absence of a commonly accepted standard understanding of empirical truth, meaning that the truth has become what target audiences can be convinced about. A dramatic increase in volumes has naturally deteriorated the quality of information. As a result, expertise and science have lost their ability to convince as they have dissolved in the ocean of easily digestible and emotionally compelling information. The phenomenon of alternative facts has, in turn, facilitated the creation of so-called information bubbles, which is a community of information consumers united around information sources based on their pre-set shared beliefs. The paradox of coexistence of more than one truth has created a fertile ground for the rise of fake news, disinformation and conspiracy theories, eventually resulting in a deeply fragmented and polarised information environment. Enabled and bolstered by the unlimited possibilities of

cyberspace, information warfare has grown to be the most potent tool of hybrid warfare, challenging the cohesion of Euro-Atlantic alliances, institutions and societies.

Expansion of internet access worldwide, availability of mobile technologies and the social media boom have facilitated an unprecedented multiplicity of sources, often providing contradictory information to information consumers – the people. Everyone with a smartphone and internet connection can be a source of information and an author, empowered with a chance to attract the attention of millions in one click. The role of social media in today's information environment cannot be overestimated, with >2.5 billion active Facebook users, around 6 billion videos viewed daily on YouTube, almost 1.5 billion daily TikTok downloads and >75 million pictures uploaded daily on Instagram (Internet Live Stats, 2020). Authoritarian regimes effectively utilise social media platforms for the manipulation of internal and external audiences. Hordes of internet trolls and botnets – fake social media accounts creating and multiplying disinformation narratives – are deliberately targeting public opinion to sow discord, inflict divides, confuse societies and obstruct democratic processes. This, in turn, has resulted in the 'weaponisation' of information as individuals and groups of people become targets or stakeholders in information warfare.

Authoritarian regimes, Russia in particular, have learned how to take advantage of the vulnerabilities and use the fundamental principles of democracy to undermine democracy itself. By hiding under the umbrella of freedom of expression, Russia's state-funded disinformation tools, such as Russia Today and Sputnik, are exploiting the weaknesses of societies across the Atlantic. The efforts of the mainstream disinformation sources largely reinforce social media campaigns with the shared goal to inflict and widen divides in democratic societies, as well as to empower radical and extremist groups. Regardless of the specific political beliefs or orientation, the Kremlin supports all ultra movements on the extreme left or extreme right, turning a traditional political rainbow into a fire loop (Győri & Krekó, 2016). Based on specific objectives in different contexts, Russian information warfare structurally involves political proxies and agents of influence in the process of building and spreading various pro-Russian and anti-Western information campaigns. In many cases, information warfare tactics boil down to turning the genuine grievances and vulnerabilities within the democratic societies into an opportunity for populist leaders, not necessarily to argue who is right and who is wrong, but just for muddying the water and raising issues for future information campaigns.

In addition to the offensive information warfare strategies, authoritarian regimes pay particular attention to so-called defensive or preventive measures to protect their own information environments from foreign interference and proliferation. The information security doctrine of Russia openly states that the 'national security of the Russian Federation substantially depends on the level of information security' (President of Russia, 2008). In practice, this policy is translated into measures aimed at securing the centre of gravity of revisionist Russia – survival and consolidation of the regime. Specific measures are aimed at total control of the information ecosystem and brutal oppression of the opposition views in the political and civil society sectors. Control of the narrative for internal audiences and censorship of information is Russia's heritage from the Soviet Union on the one hand and a link to other authoritarian regimes on the other. Based on a shared vision on information security policy, Russia and China heavily rely on information warfare to influence public opinion and to pressure democratic processes at home and abroad.

Authoritarian regimes recognise effective control of cyberspace and the information environment as a vital part of their overall revisionist strategies. With the 'great firewall' policy, China blocks access to unfavourable foreign websites and even localises internet traffic within national borders more effectively than Russia (Bloomberg, 2018). While China has long deployed aggressive censorship, propaganda and information manipulation efforts within its borders, information operations directed at foreign audiences have generally focussed on positively framing itself. In contrast to Russia, China also concentrates a significant part of its external narratives on promoting its positive image or to cover up the government's controversial actions, such as violence against protesters in Hong Kong in 2019 or the existence of Uighur detention camps (Watts, 2020). However, an essential commonality between Russian and Chinese doctrines is that there is no clear distinction between cybersecurity and information security policies. Consequently, both Russia and China clearly see cyberspace as an information domain and try to effectively utilise it as an enabler of both defensive and offensive information warfare strategies.

3 Contemporary security environment and future trends in the times of pandemics

By 4 June 2020, there have been 6,575,177 confirmed COVID-19 cases, with 388,060 deaths around the globe (WorldoMeter, 2020). This pandemic, in a matter of months, has affected all continents, all countries and all regions. It has threatened the lives of every person regardless of race, sex, age or status. Since the beginning of the writing of this article, the situation has significantly improved and the peaks of the spread and fatalities are already behind in the Euro-Atlantic area. The total panic in societies is slowly being overcome, and many governments are carefully easing restrictions. Still, the pandemic is present, and there is no indication about fundamental variables such as how long the pandemic will last, will there be a second wave and when there will be an effective treatment or vaccine available. Without a doubt, this global crisis will trigger geopolitical changes of some scale and will affect the security environment in particular. Global confusion surrounding pandemics will probably exacerbate such vulnerabilities as transatlantic and European divides, which in turn will provide revisionist powers with broader opportunities to wage hybrid warfare.

With too many unknowns surrounding COVID-19, it is difficult to predict the consequences of the pandemic. However, there are already some visible trends, which provide specific evidence for analysis. The expert community already is in a position to combine facts and evidence with historical experiences and thus develop analysis beyond the educated guess. Leading opinion makers and experts surveyed for this specific research seem to agree on the ongoing trends and the analyses of factors affecting Euro-Atlantic security, specifically in relation to the pandemic crisis. While the answers to the survey questions contain valuable and exclusive viewpoints, in surprisingly many cases, the surveyed experts agree in their analysis. There is more diversity in terms of conclusions that experts draw from the analysis of the current situation. The survey shows that the outbreak of COVID-19 has raised questions regarding the future of the world order more broadly and especially regarding the role of hybrid warfare in the times of pandemics.

As Russian political ideologist Aleksandr Dugin was hoping even before the pandemic, the COVID-19 outbreak and the urgent need for physical survival have led states to abandon liberal and transnational approaches (Memri, 2020). The fact is that in search of solutions to the global problem, the states have had to prioritise the interests of the nation-state by locking inside national borders. Dugin's main argument is that all the institutions, all the mechanisms and even the ideas of globalism, liberalism and a common vision of full transparency have utterly failed to prevent spread or to respond to the pandemic. Moreover, he argues that adequate handling of the crisis was only possible through closure of borders and restricting fundamental freedoms. This brings him to the conclusion that the pandemic has precipitated the inevitable win of the revisionist regimes and that democracies will gradually deteriorate, as already demonstrated in some Western countries, such as Hungary. Finally, Dugin generalises the exceptional conditions of the global pandemic in contemporary geopolitics to suggest that there will be no going back to globalism and that the world has already turned multipolar. What Dugin regards as a multipolar world has been discussed among security experts as possible regionalisation in the aftermath of COVID-19. There is an obvious gap on how different powers understand the process and the expected outcomes of regionalisation. The revisionist understanding of the regionalisation obviously implies legitimation of the spheres of exclusive influence in their neighbourhoods. From the Western side, there is hope that regionalisation will happen at the expense of China through the consolidation of transatlantic efforts and the decoupling of dependence on Chinese supply channels and markets.

Wide differences between the revisionist powers and the West on the future of the global world order are now as obvious as ever. In contrast to Dugin's conclusions, Professor Joseph Nye of Harvard University argues that the COVID-19 crisis will not be enough to replace existing world order (Nye, 2020). While acknowledging inevitable change, he is more sceptical of the idea that the pandemic will bring a completely new post-globalisation reality. Nye defines the key factor of globalisation as interdependence across the continents facilitated by the breakthrough in transportation and communication technology. He concludes that 'walls, weapons, and tariffs' cannot stop the transnational effects of these essential aspects (Nye, 2020). However, Nye admits that aspects of globalisation affected by governments' policies, such as the economy, will certainly be curtailed. Still, while not mentioning Russia as a global power at all, Nye's key point is that China is not even close to surpassing the US in the worldwide power competition. His calculations are based on a couple of vital criteria, such as the ability to use soft power and forge alliances, openness to attract the world's talent and influence in international institutions. More specifically, he concludes that as both economies have been struck, the US is still much better off in terms of energy resources, technology, demographic situation and

the quality of education. The combination of these factors leads Nye to the conclusion that it is too early to predict a geopolitical turning point.

The first and more general question of the survey designed for this study was aimed at collecting expert opinions specifically on the impact of COVID-19 on the security environment in the Euro-Atlantic area. The question provided three options for a multiple-choice question and an additional section with the follow-up question. More than half of the surveyed experts think the security environment in the Euro-Atlantic area will deteriorate significantly after the pandemic. Ten experts have chosen the option 'likely', against seven choosing 'neither likely nor unlikely' and only one choosing 'likely'. In additional comments, most of the experts expressed their concern that the sense of collective identity, common interests, coherence and solidarity will be deteriorating between and within Euro-Atlantic Allies in the aftermath of the pandemic. Two experts argued that the inadequate response and leadership failure by the US administration have jeopardised the security of the Euro–Atlantic area by allowing China and Russia to exploit the void. Consequently, they connect the survival of the transatlantic partnership with President Trump's departure from the Oval Office after the upcoming presidential elections in the US.

A second question of the expert survey was aimed at measuring experts' perception about the possible transformation of the threats and challenges to Euro-Atlantic security after the COVID-19 crisis. This question also provided three options for a multiple-choice question and an additional section with the follow-up question. With seven choices per option, an equal number of experts think that the transformation of threats and challenges to the Euro-Atlantic security is 'likely' or 'neither likely nor unlikely'. In the opinion of four experts, the threats and challenges are unlikely to transform after the COVID-19 crisis. The mainstream idea in the experts' comments was that the threats would not change. The expected changes are more related to the ways in which the Euro-Atlantic community will jointly deal with the threats and with building resilience against similar challenges in the future. The majority of experts indicate the fear of rise in authoritarianism and the threat of revisionist regimes becoming even more destructive. One expert specifically mentioned that the Russian threat will be as toxic as ever; however, the pandemic will push China to be more aggressive in the international arena. Other experts note that even Russia might become more assertive and engage more intensively in conflicts in its neighbourhood or in the Middle East directly or through proxies. However, the prevailing expert opinion argues that neither Russia nor China will be in the position to afford an arms race with the US; consequently, they will still heavily rely on hybrid strategies.

Many experts reiterated that the post-pandemic crisis would strike everyone and the defence sectors will suffer financial cuts in every part of the world. At the same time, the experts acknowledge that authoritarian regimes have more liberty in decision-making as they are less bound by public opinion and social grievances. One expert points to recent historical examples when Russia exploited the West's attention being consumed by the Ukraine crisis to engage in Syria. Another example is how Russia used the invasion of Georgia to distract its own people's attention from socioeconomic hardships for creating and financing a massive military modernisation programme. Luke Coffey, from the Heritage Foundation, USA, notes that a drop in oil prices and the apparent mishandling of the pandemic might put pressure on Putin's internal popular rating and legitimacy, which in turn might push him towards more aggressive foreign actions. Other experts also mention this possibility, labelled as 'rally society behind the flag'. The majority of experts indicate the trend of intensification of non-traditional and hybrid threats after the pandemic. Some experts indicate that to cover up gaps in military capabilities, authoritarian regimes will probably increase projection of power both at home and abroad.

3.1 Post-pandemic vulnerabilities in the Euro-Atlantic area

Whether globalisation will be hampered and replaced by a multipolar world in the post-corona times remains to be seen. Much will depend on which powers will adapt to the realities best and will take the leadership role in overcoming the global crisis. The leadership role of the West and how the US and the EU will handle the crisis will be crucial for the survival of the rules-based, liberal international system. At this point, an overly national approach and a very moderate role of the EU in handling the crisis in European states suggest that the differences and divides within the EU will probably persist and grow in the times of selfishness, inward-looking policies and financial hardships. As Francoise Heisbourg, the senior adviser to the International Institute for Strategic Studies, puts it, the crisis has strengthened the 20th-century understanding of the nation-state. He observes the trend of a state making a comeback as a protector

of the society from a foreign threat, allocator of resources and an economic manager (Heisbourg, 2020). On the other hand, the Chairperson of the Munich Security Conference, Wolfgang Iscinger, is optimistic about the opportunities to capitalise on the pandemic to make historical changes within the EU (Herszenhorn, 2020). To strengthen the EU's ability to speak in one voice, his proposal aims to transform the Union's consensual decision-making into a majority vote on foreign- and security-related issues. Ischinger also supports the new Franco-German plan to issue a common debt of 500 million Euros as a coronavirus recovery fund, which – in his understanding – would strengthen the EU's standing as a global power. Another important indication about the vision of global geopolitics is the recently announced slogan of Germany's upcoming presidency of the Council from July 2020: 'Together. Making Europe strong again' (Posner & der Burchard, 2020). The Germany-led initiatives are very timely and important in terms of strengthening the EU's cohesion and its standing as a global power. However, while strengthening the Union from within, the risk of harming the already-troubled transatlantic relations should not be underestimated.

The trends already show that there will be a worldwide economic recession. During the 2007–2009 international financial crisis, the main impact was brought about by the combination of recession in the private sector of the European states, with reduced production, rising unemployment and home mortgage delinquencies (Cervera, 2012); factors that will probably be even worse given the much higher scale of the ongoing economic shutdown. Based on the projections of the International Monetary Fund (IMF, 2020), the average recession for the year 2020 in the European area will be 7%–9%. Analysis of the previous large-scale economic crisis has shown a clear tendency of cutting defence expenditures, especially in Western countries (European Parliament, 2011). Reduced defence budgets will put additional pressure on the development of autonomous or sovereign European defence capabilities. On the one hand, this will once again emphasise the indispensable role of NATO in ensuring Euro-Atlantic security and stability. On the other hand, the high possibility of European states abandoning NATO's benchmark of spending 2% of gross domestic product (GDP) on defence will inevitably add tensions to the transatlantic relations. An interesting fact is that since the UK has left the EU, >80% of the defence expenditures of the NATO Allies come from non-EU member-states[6] (NATO, 2019). At this point, NATO–EU cooperation in reinforcing each other's efforts in boosting Euro-Atlantic resilience, instead of investing in overlapping capabilities, seems most timely and urgent.

At this point, trends show that the pandemic is aggravating the greatest vulnerability of the West by rubbing salt into the transatlantic wound. Two controversial decisions of the US administration have not contributed to building trust across the Atlantic – closing borders with European Allies without prior consultations and withdrawal of the funding for the World Health Organization (WHO) in the middle of the pandemic. The US inaction on the global stage has created a huge vacuum for the revisionist powers to promote their policies and narratives through the so-called 'mask diplomacy'. For example, China and Russia have been sending humanitarian aid packages with medical equipment of questionable quality to several Western countries and their allies, which has created a controversial context about the political intentions of the aid (O'Connell, 2020). So far, despite the ongoing lively deliberations in Brussels about the EU's common stance on cooperation opportunities with the US and China, there is no indication that the 'mask diplomacy' has positively changed European perceptions of any revisionist power. At the webinar organised by Globesec, Nathalie Tocci – special advisor to the Vice President of the European Commission – has stressed that the EU needs to find 'internal glue' to resist the global power competition of the US and China (Globesec, 2020). The conclusions of the webinar with the self-explanatory topic of 'Europe (Un)Divided? Southern & CEE States' Post-Pandemic Position' suggest that the EU itself will not be in a position to play the role of a global power in today's increasingly confrontational world. The mere fact that the US and China are discussed in similar contexts in the EU shows the poor state or prospects of transatlantic relations. At this stage, the global competition is free from real substance. The powers are locked in the battle for narratives on who is to blame for the inception and the spread of the pandemic and who is better at handling the crisis. Ultimately, the real leadership role would be demonstrated in the ability of the powers to compete in finding comprehensive solutions, such as vaccines or treatment on the one hand and real recovery programmes on the other.

The question in the expert survey addressing the effect of COVID-19 on transatlantic relations provided five options for a multiple-choice question and an additional section with the follow-up question. Eleven experts chose that COVID-19 will negatively affect transatlantic relations, while five marked 'neutral', against one vote for each 'positive' and 'very negative' option. Interestingly, while all 18 experts provided comments to most of the other questions, the current question received only one clear and symptomatic answer: "differences across the Atlantic will grow". However, many

6 Non-EU members of NATO: the US, the UK, Turkey, Canada, Norway, Montenegro, Albania and North Macedonia.

experts covered specific comments related to the transatlantic relation while commenting on other questions of the survey. Another question focussed on the expected effect of COVID-19 on the unity of the EU in general and the common security and defence policy in particular. The question provided five options for a multiple-choice question and an additional section with the follow-up question. Altogether, 12 experts responded that the effect of COVID-19 on the EU would be 'negative', while three chose the 'neutral'. One vote each went to 'very positive', 'positive' and 'very negative' options. In contrast to the previous question, 15 experts provided their comments to this question.

Many experts express concern that the fragmentation and differences within the EU would probably grow as a result of the crisis. UK-based researcher Illya Roubanis points out explicitly that COVID-19 could deepen the cleavages between net contributors to and net beneficiaries from the EU budget, in addition to accelerating the North–South division. Other experts also hinted at the risk of more divergence between member states' threat perceptions and security policy priorities. Egor Kuroptev from the New Russia Foundation, supported by one other expert, explains that he answered 'very positive' because the pandemic has revealed the structural deficiencies and apparent vulnerabilities of the West, which in itself provides an excellent opportunity to learn lessons and build resilience according to the revealed shortcomings. However, other experts fear that the early response to COVID-19 has already turned EU member states inwards, and solidarity will be the victim of the process. Retorting partially to the issue of transatlantic relations, a few experts believe that the leadership role of the US in responding to the crisis will also largely determine processes within the EU. One comment mentions the change of the US administration during the next elections explicitly as a defining factor for transatlantic cohesion, in turn largely affecting the solidarity within the EU. In his final comment, Luke Coffey also touches upon the importance of transatlantic unity not only for purely security purposes but also for economic recovery from the COVID-19 global crisis. Notably, many experts used the final comments section to emphasise distrust, polarisation and lack of unity within and among Western countries as the critical vulnerability. Experts share fears that the mentioned vulnerabilities equally strengthen right-wing nationalism and radical leftist movements, generating public support to populism, disinformation and conspiracy theories.

3.2 Pandemic hybridity

One of the questions of the expert survey focussed specifically on the new opportunities for Russia and China to challenge the liberal world order and to accelerate hybrid warfare against the West. The question provided three options for a multiple-choice question and an additional section with the follow-up question. Going into more details of the hybrid warfare tools, 12 experts responded that the pandemic presented more opportunities to Russia and China to harm Western interests. Five experts responded that the growth of threats was 'neither likely nor unlikely', with only one optimistic viewpoint choosing 'unlikely'. The comments of all five experts who marked intermediary option reveal that they do not underestimate the threat of more assertive hybrid warfare by the revisionist powers in the post-pandemic period. Instead, they indicate that both Russia and China are already very effectively using hybrid warfare to advance their revisionist objectives. The core of the argument of an expert choosing the option 'unlikely' is that revisionist powers will be hit hard by the COVID-19 crisis, as hard as the Western. Thus, especially Russia, who is dependent on drastically reduced oil revenues, will be deprived of the opportunities to accelerate hybrid warfare. However, even this comment clearly indicates that the reliance on information warfare and using Western cohesion as vulnerability will persist in the future.

Another concern commonly expressed in the expert survey was that economic and financial difficulties might shift the attention of the governments in the Euro-Atlantic area away from defence and security. It was mentioned in the comments that this trend would deteriorate the security environment and create more opportunities for Russia and China to increase influence in the Euro-Atlantic area. A specific worry related to poor financing of the security sector is the degrading appetite for security cooperation projects, leaving more space for revisionist interest. Another dominant expert opinion underlines the point of the increased importance of boosting resilience against non-kinetic tools of hybrid influence in times of military stagnation. One expert expects to keep current status-quo in modernisation, procurement and innovation, because the limitation on defence spending will affect the West and its adversaries in a balanced manner. Another expert elaborates further by arguing that reduced demand for defence equipment could affect production and supply chains in defence industries. Two comments focussed attention on the importance of supply chain and markets being diversified from China, specifically for defence and security purposes.

Authoritarian regimes are historically less reluctant in cutting military expenditures during crises as they experience less pressure from public opinion in times of socioeconomic difficulties (European Parliament, 2011). This time, due to the unprecedented trajectory of the oil prices, Russian defence plans might come under more pressure (Waller, 2020). Forbes's report points to specific indications that the Chinese economy will suffer significantly from a number of Western companies abandoning Chinese supply chains and leaving the market (Rapoza, 2020). A long-standing debate about the security aspects of business relations with China, in general, and of China's domination in 5G technology, in particular, has become more urgent during the pandemic. A positive development, giving a good example to other Western countries, is Canada's decision to ditch Huawei and team up with European Ericsson and Nokia in building 5G telecom networks (Warburton & Malara, 2020). NATO Secretary General Stoltenberg seems to expect rising tensions and elevated threats not only from Russia but increasingly also from China: 'The rise of China is fundamentally shifting the global balance of power… multiplying the threats to open societies and individual freedoms and increasing the competition over our values and our way of life' (Rettman, 2020). An important development, which will significantly affect the Euro-Atlantic security environment, is that there is a visible trend that authoritarian regimes will synchronise and coordinate their hybrid warfare against Western interests and values.

3.3 Hybrid challenge to democracy

The point on vulnerabilities such as divisions and uncertainty in democratic societies presenting a powerful weapon to revisionists is duly noted in the vast majority of comments in the survey. Experts almost unanimously underline transatlantic cohesion and public trust towards European values and interests as the centre of gravity targeted by the disinformation and propaganda campaigns of the revisionists. One comment specifically focussed on the attempts of the revisionists to apply soft power, taking advantage of the distractions caused by the pandemic. Without spelling out explicitly, the comment meant to argue that the humanitarian aid sent to Western countries by China and Russia was part of the propaganda campaigns that tried to cover up their own deficiencies in responding to the pandemic. Some experts have already identified the trends of Russia and China trying to take advantage of the global confusion and the crisis to promote their political agendas, specifically through utilising information space against democracy. For the first time, experts see the authoritarian regimes joining forces in orchestrated information strategies and campaigns.

A recent report of the German Marshall Fund of the US (GMF) identifies an exceptional trend evidenced during the COVID-19 crisis – the first time that an authoritarian anti-Western coalition has been formed by Russia, China and even Iran (Watts, 2020). The trend clearly shows China resorting to classical Russian strategy – Chinese fake social media accounts and bots, with the assistance of state-controlled media outlets, 'have promoted multiple and at times conflicting' disinformation and conspiracy theories. According to the report, Iran and Russia are reinforcing China's information campaigns by multiplying Chinese narratives through their own channels, claiming that the coronavirus is an American bioweapon, as well as with other misinformation 'that further confuses world audiences about the origin, advance, containment, and treatment of coronavirus'. There are also reports that authoritarian regimes have exploited the pandemic crisis to exert even more control over the domestic information ecosystems. In this case, Russia is learning lessons from China as both countries aggressively impose digital surveillance systems, such as contact-tracking applications, for the full control of societies in the so-called 'cyber Gulags' (Ilyushina, 2020). A powerful signal on Western countermeasures against growing authoritarian presence in the information environment is the decision to remove state-controlled media from Facebook. Acknowledging the role of social media in the manipulation of public opinion in the post-COVID-19 information space, specifically in the context of elections, Facebook has begun blocking advertisements from the television network Russia Today and news agency Sputnik of Russia as well as Chinese CCTV and Xinhua News (Gleicher, 2020). The company has developed definitions and policy on labelling 'state-controlled media', which extends beyond 'just assessing financial control or ownership and includes an assessment of editorial control exerted by a government'. The trends and evidence presented above provide the bases for the assumption that the authoritarian regimes will more aggressively utilise cyberspace to enable hybrid warfare with the aim of controlling the information environment at home and abroad.

Five of the 18 surveyed experts specifically brought up the issue that the pandemic underlined the importance of cyberspace in terms of the uninterrupted functioning of society. Egon Kuroptev brings up the specific example of Russian media holding Sputnik signing a contract with the Chinese holding Global Times to undertake massive waves

of anti-democratic and anti-Western campaigns jointly. Some of the other experts also agree that humanitarian aid was part of a broader battle for narratives to burnish the tainted image of the revisionists and boost their role as responsible global powers. One specific comment concludes that anti-establishment and Euro-sceptic groups will capitalise on the inefficient management of the COVID crisis by Western institutions and will become more influential in the aftermath of a pandemic. As a result, the deeply divided West will be more vulnerable to Russia's hybrid influence through information warfare, manipulation of public opinion and interference attempts during elections. Meanwhile, China will try to attack the transatlantic cohesion by isolating the US and the EU by pushing attractive bilateral deals with individual states, including on 5G through the Digital Silk Road initiative. Experts expressed concern that aggressive restrictions and disruption of global interaction might affect the state of democracy around the world. The lockdown might generate a short-term deficit of public acceptance and a populist retrenchment stemming from deterioration of some individual freedoms such as freedom of movement and privacy. However, the trend in the expert opinions shows that despite the increased mistrust and hardships, a rapid change in the global security architecture is not expected. Experts still think that the pandemic will probably reinforce some of the existing hybrid threats, but it will not create an entirely new dynamic in the security area.

4 Summary and conclusions

COVID-19 is neither a revolution or turning point, nor definitely World War III. However, this global crisis has accelerated and amplified some of the already-existing trends in the security environment, such as the growing importance of hybrid warfare. Contemporary competition for global power has turned the world into a hybrid battlefield. In this modern battlefield, the strategic advantage of the authoritarian regimes in terms of being irresponsible, reckless and aggressive is balanced with the virtue of finding cheap and effective – short of war – solutions for achieving geopolitical objectives. This puts Western institutions under pressure to adapt to the current security environment quickly and effectively. The adaptation by and large implies building resilience against the continuous application of various hybrid strategies. Revisionist powers shape and adjust their hybrid strategies based on the specific opportunities that arise from Western vulnerabilities. Building resilience has become a vital component of security as it is hardly possible to fully deter, counter or defend against random hybrid threats.

It is clear that the modern hybrid battlefield will be dominated through the cyberspace and information environments. The security environment will be affected by the growing dependency of the global powers on technology and the internet. Further boosting of the hybrid warfare will largely define the security environment in the Euro-Atlantic area after the COVID-19 crisis. The trend of eroding boundaries between war and peace, cyber and real, truth and falsity will persist or probably grow. The revisionist powers will continue to constantly exploit the vulnerabilities of the West and will use growing divides between and within Western countries to push a final assault against the rules-based international system. The expert community seems to agree that the pandemic might hamper the globalisation process and encourage regionalisation. The revisionist vision of the so-called 'regionalisation' actually means that global powers will be taking care of the spheres of influence in the regions around them. Russia and China are fighting for replacing the US hegemony with a multipolar world order, wherein they will be allowed to promote their national interests at the expense of other countries in the neighbourhood.

Massive disruption of connectivity and the lockdown of economic activity will inevitably translate into severe global recession in all parts of the world. It looks like new divides in the West will be stemming from economic recession and financial hardships in the post-pandemic times, as well as from the lack of common vision on an adequate response to the far-reaching effects of the crisis. Disengagement on defence- and security-related issues within NATO and EU will deepen due to the availability of fewer resources. Fair burden sharing, an important criterion of the transatlantic cohesion for the current US administration, will be more problematic. The already-inward-looking policies and the evident failure of the US to lead during the global crisis, in combination with the European push towards more autonomy, might irreparably damage transatlantic relations.

The pandemic crisis has hit Western countries, as well as revisionist powers, hard. However, authoritarian regimes have a certain advantage in responding to the crisis due to the lack of transparency and accountability while imposing restrictions and limitations on their societies. While democratic leaders have gained more powers through state

emergency laws, they are still limited in decision-making options even during the pandemics. Authoritarian regimes have exploited the pandemic to strengthen positions internally through the imposition of new control and surveillance systems over populations, while similar attempts in some democratic countries have triggered the rollback of democracy and further damaged Western cohesion.

Both Russia and, increasingly, China have conducted active information campaigns at home and abroad in an attempt to boost their image as responsible global powers on the one hand and to challenge Western unity on the other. Since the outbreak of a battle for narratives on the genesis and features of the pandemic, China's new disinformation pattern evolved to include an aggressive offensive against the US using Russia-style information campaigns. These multicomponent campaigns combine a wide variety of state-controlled media outlets, troll factories and botnets. A monumental shift in the information landscape is the authoritarian coalition in which China and Russia are engaging with other authoritarian regimes towards their revisionist ends. The coalition is trying to capitalise on the estrangement in the Western world and fuel anti-Western sentiment, Euro-scepticism, nationalism and xenophobia.

Today, when less money is available for military spending, the cost-effective solutions offered by hybrid warfare through cyber and information operations seem to be the obvious choice. It has become a widely acknowledged fact that revisionists have found effective ways of utilising hybrid warfare as the most powerful weapon against democracy. There is a consensus among security experts that the unprecedented boost of the cyberspace and information ecosystem, in terms of their size, importance and sophistication, has allowed hybrid warfare to become a defining factor of the contemporary security environment. The COVID-19 pandemic, while touching every aspect of the lifestyle of modern societies, has precipitated some of the tendencies such as the rush of governmental, business-related, educational and all other socioeconomic operations and services into the cyberspace. This trend will boost the importance of cyber effects and cybersecurity considerations for all world powers. Victory in the global power competition now obviously lies in the ability to dominate the cyberspace and information environment.

It is now safe to assume that there is an urgent need for the West to consolidate around common values and interests to avoid the collapse of the global system. The West should enhance its resilience by bridging the gaps in common threat perceptions on the one hand and build common vision and strategy on the other. NATO and the EU provide perfect frameworks to be filled with meaningful content. Euro-Atlantic institutions are well equipped with the tools that promote international cooperation with the aim of strengthening common values and interests. An obvious takeaway from the still-evolving global crisis is that not a single country or institution is adequately equipped to respond to modern threats. With every healthcare and crisis management system in the world failing to adequately counter or respond to COVID-19, it is now the right time to re-evaluate vulnerabilities and invest in the resilience of the Euro-Atlantic security.

Annexe 1

List of surveyed experts[7]

1. Mirian Popkhadze, Fellow at the Foreign Policy Research Institute; Completed on 24/5/2020
2. Iftah Burman, Bar Ilan University, Middle East Department; Completed on 19/5/2020
3. David Ucko, National Defense University; Completed on 18/5/2020
4. Tomas Jermalavičius, International Centre for Defence Studies (ICDS); Completed on 18/5/2020
5. Luke Coffey, The Heritage Foundation; Completed on 18/5/2020
6. Egor Kuroptev, Free Russia Foundation; Completed on 15/5/2020
7. Anonymous expert from Estonia; Completed on 14/5/2020
8. Gustav Gressel, European Council on Foreign Relations (ECFR); Completed on 14/5/2020
9. Anonymous expert from the US; Completed on 12/5/2020
10. Steven Blockmans, Director ad interim, Centre for European Policy Studies (CEPS); Completed on 12/5/2020
11. Neil MacFarlane, University of Oxford; Completed on 7/5/2020

7 Twelve experts have chosen to be listed among the surveyed experts without attribution of specific answers, three stayed anonymous and another three allowed full disclosure.

12. Misha Darchiashvili - Former Deputy Defence Minister of Georgia; Completed on 7/5/2020
13. Colonel Jean Trudel, Canadian Armed Forces, Baltic Defence College; Completed on 7/5/2020
14. Ambassador Alex Petriashvili; Completed on 6/5/2020
15. Dr Ilya Roubanis, Government Affairs Consultant; Completed on 6/5/2020
16. Dr Asta Maskaliunaite, Baltic Defence College; Completed on 6/5/2020
17. Ambassador Batu Kutelia, Vice President, Atlantic Council of Georgia; Completed on 6/5/2020
18. Anonymous expert from Georgia; Completed on 6/5/2020

Annexe 2

Survey questions

How will the COVID-19 pandemic change the security environment in the Euro-Atlantic area?

Q1: Will COVID-19 have a significant impact on the security environment in the Euro-Atlantic area?[8]
- Please specify the main variables of the Euro-Atlantic security that could be affected by the COVID-19 crisis

Q2: Will the threats and challenges to the Euro-Atlantic security transform after the COVID-19 crisis?
- Please specify which specific threats might be affected in positive or negative ways

Q3: Will the COVID-19 crisis open new opportunities for Russia and China to challenge the liberal world order and to accelerate hybrid warfare against the West?
- Please elaborate on how revisionist regimes might exploit the pandemic crisis to their advantage

Q4: How will economic recession, financial crisis and energy markets in the post-COVID-19 period affect the defence and security sectors of the major Western military powers (the US, the UK, France and Germany)?

Q5: How will economic recession, financial crisis and energy markets in the post-COVID-19 period affect the defence and security sectors of the revisionist regimes (Russia, China)?

Q6: How will COVID-19 affect transatlantic relations?

Q7: How will COVID-19 affect the unity of the EU in general and the common security and defence policy in particular?
- Please specify the main factors that will drive the EU's internal dynamics on issues related to defence and security

Q8: Please, share any comments/remarks you might have regarding the impact of the COVID-19 crisis on the aspects of our lives not mentioned in the questions above.

Q9: How can we refer to the information provided by you?

Bibliography

Aris, B. & Tkachev, I., 2019. *Long Read: 20 Years of Russia's Economy Under Putin, in Numbers.* [Online] Available at: https://www.themoscowtimes.com/2019/08/19/long-read-russias-economy-under-putin-in-numbers-a66924 [Accessed 03 June 2020].

Bloomberg, 2018. *The Great Firewall of China.* [Online] Available at: https://www.bloomberg.com/quicktake/great-firewall-of-china [Accessed 03 June 2020].

Cervera, R., 2012. Impact of the Economic Crisis on Defence Policies: a Comparative Study. *Journal of the Higher School of National Defense Studies,* Volume 0.

CISA, 2009. *Official website of the Department of Homeland Security.* [Online] Available at: https://www.cisa.gov/national-strategy-secure-cyberspace [Accessed 9 June 2020].

European Parliament, 2011. *The Impact of the Financial Crisis.* [Online] Available at: https://www.europarl.europa.eu/document/activities/cont/201106/20110623ATT22406/20110623ATT22406EN.pdf [Accessed 09 June 2020].

FCO, 2020. *Press Release: UK condemns Russia's GRU over Georgia cyber-attacks.* [Online] Available at: https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks [Accessed 03 June 2020].

Gleicher, N., 2020. *Labeling State-Controlled Media On Facebook.* [Online] Available at: https://about.fb.com/news/2020/06/labeling-state-controlled-media/

8 The criterion of the adjective 'significant' was not predefined in the survey; thus, the experts provided their views based on the general understanding of the word.

Globesec, 2020. *Europe (Un)Divided? Southern and CEE States' Post-Pandemic Position.* [Online] Available at: https://www.facebook.com/GLOBSECforum/videos/306965516976013/ [Accessed 09 June 2020].

Goldman, A., Barnes, J. E., Habermann, M. & Fandos, N., 2020. *Lawmakers Are Warned That Russia Is Meddling to Re-elect Trump.* [Online] Available at: https://www.nytimes.com/2020/02/20/us/politics/russian-interference-trump-democrats.html [Accessed 03 June 2020].

Győri, L. & Krekó, P., 2016. *open democracy.* [Online] Available at: https://www.opendemocracy.net/en/odr/don-t-ignore-left-connections-between-europe-s-radical-left-and-ru/ [Accessed 9 June 2020].

Heisbourg, F., 2020. From Wuhan to the World: How the Pandemic Will Reshape Geopolitics. *Survival,* 62(3), pp. 7-24.

Herszenhorn, D. M., 2020. Ischinger: German-French recovery plan could transform EU and seal Merkel's legacy. *Politico*, 19 May.

Hormats, R., 2020. *World War III isn't what the strategists thought it would be.* [Online] Available at: https://thehill.com/opinion/national-security/492409-world-war-iii-isnt-what-the-strategists-thought-it-would-be [Accessed 03 June 2020].

Ilyushina, M., 2020. *Moscow rolls out digital tracking to enforce lockdown. Critics dub it a 'cyber Gulag'.* [Online] Available at: https://edition.cnn.com/2020/04/14/world/moscow-cyber-tracking-qr-code-intl/index.html

IMF, 2020. *World Economic Outlook, April 2020: The Great Lockdown.* [Online] Available at: https://www.imf.org/en/Publications/WEO/Issues/2020/04/14/weo-april-2020

Internet Live Stats, 2020. *Internet Live Stats.* [Online] Available at: https://www.internetlivestats.com/ [Accessed 04 June 2020].

Jinghua, L., 2019. *What Are China's Cyber Capabilities and Intentions?.* [Online] Available at: https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734 [Accessed 03 June 2020].

Li, X. & Shaw, M. T., 2014. ame Bed, Different Dreams" and "Riding Tiger"Dilemmas: China's Rise and InternationalRelations/Political Economy [Data table "Real GDP in the U.S. and China, 1980-2030"]. *Journal of Chinese Political Science*, 15 January, Volume 19, pp. 69-93.

Mandelbaum, M., 2019. The New Containment: Handling Russia, China, and Iran. *Foreign Affairs*, March/April, Volume 98, p. 123.

McIntyre, L., 2018. *Post-Truth.* Cambridge Massachusetts: MIT Press.

Memri, 2020. Anti-Liberal Russian Philosopher Dugin: The New Multi-Polar World Order Is Upon Us, Where Russia, China And Even The United States, Can Survive By Suspending Democracy. *Memri, Special Dispatch*, 22 April.

Merriam-Webster, 2020. *Unpeace, nown.* [Online] Available at: https://www.merriam-webster.com/dictionary/unpeace [Accessed 03 June 2020].

NATO, 2019. *Defence Expenditure of NATO Countries (2013-2019).* [Online] Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_11/20191129_pr-2019-123-en.pdf

NCSC, 2018. *National Cyber Security Centre.* [Online] Available at: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed [Accessed 8 June 2020].

Nye, J. S., 2020. No, The Coronavirus Will Not Change the Global Order. *Foreign Policy*, 16 April.

O'Connell, K., 2020. *washingtonpost.* [Online] Available at: https://www.washingtonpost.com/outlook/2020/05/05/are-there-any-humanitarian-superpowers-covid-19-fight/ [Accessed 9 June 2020].

Paterson, T. & Hanley, L., 2020. Political warfare in the digital age: cyber subversion, information operations and 'deep fakes'. *Australian Journal of International Affairs,* March.

Pisciottta, B., 2020. Pisciotta, Barbara. "Russian revisionism in the Putin era: an overview of post-communist military interventions in Georgia, Ukraine, and Syria. *Italian Political Science Review/Rivista Italiana di Scienza Politica*, 50(1), pp. 87-106.

Posner, J. & der Burchard, H. v., 2020. Back off, Trump. Germany wants to Make Europe Strong Again. *Politico*, 05 May.

President of Russia, 2008. *Information Security Doctrine of the Russian Federation.* [Online] Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf [Accessed 03 June 2020].

Rapoza, K., 2020. *New Data Shows U.S. Companies Are Definitely Leaving China.* [Online] Available at: https://www.forbes.com/sites/kenrapoza/2020/04/07/new-data-shows-us-companies-are-definitely-leaving-china/#3e29bbe440fe

Rattray, G. J., 2001. *Strategic Warfare in Cyberspace.* Cambridge, Massachusetts/London, England: MIT Press.

Rettman, A., 2020. *Nato: China-Russia axis threatens Western power.* [Online] Available at: https://euobserver.com/foreign/148597

Reuters/Interfax, 2019. *Russian military specialists arrive in Venezuela to service equipment: Interfax.* [Online] Available at: https://www.reuters.com/article/us-russia-venezuela-specialists/russian-military-specialists-arrive-in-venezuela-to-service-equipment-interfax-idUSKBN1WA2FJ [Accessed 03 June 2020].

RFI/AFP, 2020. *World will be same but worse after 'banal' virus, says Houellebecq.* [Online] Available at: http://www.rfi.fr/en/wires/20200504-world-will-be-same-worse-after-banal-virus-says-houellebecq?ref=fb&fbclid=IwAR1_1JAt8woJ_8xehsYu8OErYh-YxW29YDLptU7vZQh9GJtPl15aG7UGhng [Accessed 06 June 2020].

Stubbs, J., Menn, J. & Bing, C., 2019. *Exclusive: China hacked eight major computer services firms in years-long attack.* [Online] Available at: https://www.reuters.com/article/us-china-cyber-cloudhopper-companies-exc/exclusive-china-hacked-eight-major-computer-services-firms-in-years-long-attack-idUSKCN1TR1D4 [Accessed 03 June 2020].

Su, J., 2019. *Warning: A Security Flaw In Kaspersky AntiVirus Lets Hackers Spy Users Online, Millions At Risk.* [Online] Available at: https://www.forbes.com/sites/jeanbaptiste/2019/08/16/warning-a-security-flaw-in-kaspersky-antivirus-lets-hackers-spy-users-online-millions-at-risk/#61aaf3f3ba34 [Accessed 03 June 2020].

Surkov, V., 2019. *Vladislav Surkov's Hugely Important New Article About What Putinism Is - Full Translation.* [Online] Available at: https://russia-insider.com/en/vladislav-surkovs-hugely-important-new-article-about-what-putinism-full-translation/ri26259 [Accessed 1 June 2020].

Tucker, P., 2019. *Russia Is Perfecting the Art of Crushing Uprisings Against Authoritarian Regimes.* [Online] Available at: https://www.defenseone.com/technology/2019/07/russia-perfecting-art-crushing-uprisings-aid-authoritarian-regimes/158396/ [Accessed 03 June 2020].

Wakefield, J., 2019. *Huawei laptop 'backdoor' flaw raises concerns.* [Online] Available at: https://www.bbc.com/news/technology-47800000 [Accessed 03 June 2020].

Waller, H., 2020. *Oil Rises After Libya Shuts Largest Field and Demand Perks Up.* [Online] Available at: https://www.bloomberg.com/news/articles/2020-06-08/oil-holds-losses-as-saudis-call-time-on-additional-output-cuts

Wang, A. B., 2016. *'Post-truth' named 2016 word of the year by Oxford Dictionaries.* [Online] Available at: https://www.washingtonpost.com/news/the-fix/wp/2016/11/16/post-truth-named-2016-word-of-the-year-by-oxford-dictionaries/ [Accessed 03 June 2020].

Warburton, M. & Malara, N., 2020. *Canadian telcos tap Ericsson, Nokia for 5G gear, ditching Huawei.* [Online] Available at: https://www.reuters.com/article/us-bell-canada-ericsson-5g/canadian-telcos-tap-ericsson-nokia-for-5g-equipment-amid-huawei-uncertainty-idUSKBN2391ZV

Watts, C., 2020. *Triad of Disinformation: How Russia, Iran, & China Ally in a Messaging War against America.* [Online] Available at: https://securingdemocracy.gmfus.org/triad-of-disinformation-how-russia-iran-china-ally-in-a-messaging-war-against-america/ [Accessed 06 June 2020].

WorldoMeter, 2020. *Coronavirus.* [Online] Available at: https://www.worldometers.info/coronavirus/ [Accessed 09 June 2020].