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

Ch. Briggs, Y. Danyk, and T. Maliarchuk
Connections QJ 20, no. 3-4 (2021): 47-72
https://doi.org/10.11610/Connections.20.3-4.03

Research Article

Security Aspects of Hybrid War, COVID-19 Pandemic and Cyber-Social Vulnerabilities

Chad Briggs,[1] Yuriy Danyk,[2] and Tamara Maliarchuk[3]

[1] *University of Alaska Anchorage, https://www.uaa.alaska.edu*

[2] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute," https://kpi.ua/en/*

[3] *NATO DEEP Working Group, https://deepportal.hq.nato.int/eacademy/*

Abstract: While developments in cyber technologies have advanced the propagation and reach of hybrid warfare, the COVID-19 pandemic has accelerated many vulnerabilities and critical dependencies. This article explores the fundamental aims and strategies of hybrid warfare in terms of psychological underpinnings and technological reach and links to emerging issues of disinformation, cybercrime, fake news, information trauma, and the influence of new modes of education on national security and state resilience.

Keywords: hybrid warfare, cyberattack, cyber security, information trauma, e-learning, emotional warfare, cognitive hacking, cyber-social vulnerabilities, cyber technologies, COVID-19.

Introduction

The concept of hybrid warfare has gained increasing attention in security and military strategy discussions, often focused on examples of Russian operations in the takeover of the Crimean Peninsula of Ukraine in 2014. As a full-spectrum approach to understanding offensive operations, ranging from social media campaigns to conventional (kinetic) warfare, the term hybrid warfare can be used to describe a wide variety of activities. Most often, the emphasis is on the irregular nature of operations, where traditional, Western understandings of conflict are masked with forces and tactics that cannot easily be traced to a state adversary.

In our previous articles, we have detailed the use of cyber technologies in carrying out a broad range of attacks on Ukraine since 2013, including specific attacks on energy infrastructure.[1] In explaining countries' vulnerabilities to the loss of control over energy supplies, one key factor was the adversary's ability to undermine public trust in institutions, i.e., when basic needs are not met, social cleavages in a country or region are worsened, and governance becomes more difficult.

That hybrid wars are currently occurring worldwide is not disputed. Countries from Russia to China have incorporated ideas of fourth-generation warfare (4GW) into military doctrine for decades, where the "red line" between peace and war dissolves and adversaries are dealt with as part of an overall strategy of asymmetric, shadow (*maskirovka*) conflict.[2] These are not wars in the traditional sense of the Hague or Geneva Conventions, with clear starting and end points, of physical occupation of territory, and with visible actors and clear intent. Hybrid wars shift across borders and can maintain a quality of permanence, attacking entire countries at times while at other times focusing on specific groups or individuals. But hybrid war actions always have a goal and marshal the resources to achieve it. Everything else is just a tool to achieve this goal in the interests of particular players (actors). The critical component is a comprehensive strategy of one actor to keep the other off balance, destabilized enough that strategic space opens for political, economic, and military actions.[3]

Hybrid wars are a kind of permanent war of variable intensity across multiple sectors, with cascading, negative impacts, and synergistic effects, in which the entire population of the country and the international community are, to a certain extent, consciously or unconsciously involved. The impacts are felt in all spheres of life, in all sectors of society, and throughout the state. Thanks to the use of innovative technologies, it has become possible to shift conflict from predominantly overt and forceful (kinetic) means to less obvious strategies focused on the structural vulnerabilities of adversaries, including by achieving cognitive advantage and control over them.

Such hybrid tactics make it possible to take control of or destabilize the basic institutions of a country and achieve strategic interests via unconventional cyber and cognitive influences (including spillover effects). Cyberspace has proven to be the main theater of asymmetric actions. It is supported by the fact that cyberspace has an extraterritorial, universal, and global character. It is also ill-adapted to national geographic borders, can serve as socializing surroundings for

---

1 Yuriy Danyk, Tamara Maliarchuk, and Chad Briggs, "Hybrid War: High-tech, Information and Cyber Conflicts," *Connections: The Quarterly Journal* 16, no. 2 (2017): 5-24, https://doi.org/10.11610/Connections.16.2.01.

2 Robert Wilkie, "Hybrid Warfare: Something Old, Not Something New," *Air & Space Power Journal* 23, no. 4 (Winter 2009): 13-18.

3 Daniel T. Lasica, *Strategic Implications of Hybrid War: A Theory of Victory* (FT Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, 2009), https://apps.dtic.mil/sti/pdfs/ADA513663.pdf.

people of nearly all ages, and is constantly expanding in scope and influence. Information flows can be realized through dialogue with mass audiences while at the same time using social media to achieve or mimic individual communication. For the time being, cyber technologies prove to be the most important instrument for shaping collective and individual consciousness and social values.

Cyber technologies, therefore, allow for hybrid strategies to realize goals of widespread impacts on society at a distance and without clear attribution to the aggressor. The most effective users of cyber-hybrid approaches determine the end effects to be realized and marshal an appropriate array of synergistic actions with overlapping, cascading, and reinforcing impacts. These impacts are focused on disabling an adversary, promoting prearranged narratives, and controlling the cognitive sphere on the emotional, moral, cultural, and mental levels. Successful actions can create a system of stable stereotypes and the perception of reality or merely foster instability and the denial of objective standards and truth.

The COVID-19 pandemic, which has ravaged the planet since December 2019, added its own peculiarities to the spectrum of hybrid confrontations and methods. It must be considered when analyzing them and making forecasts to reduce their risks and prevent and/or mitigate their consequences. This article focuses on the social nature of hybrid warfare and how technologies allow for the exploitation of social and political vulnerabilities and polarization in target states. These issues were also examined in the context of hybrid warfare, the COVID-19 pandemic, and emerging cyber-social vulnerabilities.

While attention to the military and physical infrastructure of hybrid attacks remains important, such offensive operations rely upon fragile social and political fabrics that remain integral to planning offensive strategies and appropriate defense against hybrid attacks. Historical experience has shown that hybrid warfare actions in this sphere favor the attacker – while countries such as the United States have used hybrid methods in the past to shore up political support in conflict areas, success (e.g., 1950s Philippines) is less common than failure (post-2003 Iraq or Afghanistan).[4] Particularly where an aggressor has detailed knowledge of one's opponent, social divisions are easy to exploit and have become much more vulnerable with the skillful use of cyber tools such as social media. Using examples from Ukraine and the United States, this article details ways in which technology is leveraged as an asymmetric approach to influencing and undermining an adversary's governance.

The idea of attacking the social fabric of one's adversary is hardly new. Sun-Tzu advocated attacking the morale of one's adversary and warned that protracted conflict would lower public support for wars.[5] Clausewitz likewise identified the political nature of warfare, understanding that winning a conventional

[4] Ivan Arreguin-Toft, "How to Lose a War on Terror: A Comparative Analysis of a Counterinsurgency Success and Failure," in *Understanding Victory and Defeat in Contemporary War*, ed. Jan Angstrom and Isabelle Duyvesteyn (Routledge, 2006), 160-185.

[5] Sun Tzu, "The Art of War," in *Strategic Studies: A Reader*, ed. Thomas G. Mahnken and Joseph A. Maiolo (Routledge, 2014), 86-110.

battle may not be sufficient for winning the wider war.[6] Counterinsurgency and irregular warfare experts through the 20th century were even clearer in emphasizing the importance of public morale off the traditional battlefield and pointing out that direct military force can prove to be counter-productive in winning political support in a conflict. US Air Force debates over the use of strategic bombing have been a case in point, particularly its use against civilian targets during the Second World War in Europe. While officially targeting industrial or military targets, the US approach to high-altitude bombing in Europe often resulted in high civilian casualties, with an argument (made more forcefully by the Royal Air Force) that the destruction of cities would undermine public morale and support for German aggression against the West.[7] The German Luftwaffe made similar arguments for their bombing campaign against the UK in 1940-41 and with similarly disappointing results.[8] Rather than German or British morale breaking by seeing their cities destroyed and neighbors killed by aerial bombing, the public tended to rally around their state in response to such open aggression.

Similarly, decades later, US military actions against Vietnamese villages suspected of harboring Viet Cong (VC) insurgents only seemed to increase support for the VC or at least direct public opinion against the Americans.[9] Carr argued that open violence against civilians (as opposed to the military), whether by the US military in Vietnam or the Irish Republican Army in the UK/Ireland, led to perceptions of illegitimate actions and loss of popular support among the population.[10] Yet the key ingredient in such assessments was the visibility of such actions and their clear intent. In cases where aggressive actions could be blamed on others (false flag attacks) or where the nature of the attack fell below physical violence, attribution and blame tended to fall apart.

A House Divided

The Russian military approach to warfare has long recognized the need for asymmetric approaches to conflict, meaning where an adversary's vulnerabilities would be used against it, disproportionate to the amount of force available. A common approach for Russian activities is to use influence operations, activities

---

6 Carl von Clausewitz, *On War* (Penguin UK, 1982).

7 Kenneth P. Werrell, "The Strategic Bombing of Germany in World War II: Costs and Accomplishments," *The Journal of American History* 73, no. 3 (December 1986): 702-713, https://doi.org/10.2307/1902984.

8 Edgar Jones, Robin Woolven, Bill Durodié, and Simon Wessely, "Civilian Morale During the Second World War: Responses to Air Raids Re-examined," *Social History of Medicine* 17, no. 3 (2004): 463-479, https://doi.org/10.1093/shm/17.3.463.

9 Richard Shultz, "Breaking the Will of the Enemy During the Vietnam War: The Operationalization of the Cost-Benefit Model of Counterinsurgency Warfare," *Journal of Peace Research* 15, no. 2 (June 1978): 109-129, https://doi.org/10.1177/002234337801500202.

10 Caleb Carr, *The Lessons of Terror: A History of Warfare Against Civilians* (New York: Random House, 2003).

that fall below the threshold of most military responses in Western countries and can often be masked without the aggressor admitting its activities or intentions. Influence operations are intended to use largely indirect and non-kinetic means to sow discord and division within one's adversary, relying upon pre-existing ingroup/outgroup formations to polarize politics, delegitimize the government and its institutions, and target the resilience of its population and communities to respond to outside threats.[11] While the history of influence operations is not new, cyber technologies have allowed remarkable penetration from anywhere in the world straight to individuals' computers and phones, all while masking the true source of information and disinformation.

In some military strategies, including those of the Russian Federation and China, there is a marked focus on information operations as part of larger strategies and operations, not separated as they often are in the US and Western Europe. Whether this is referred to as part of the "Revolution in Military Affairs" or other doctrines, in practical terms, these strategies refer to asymmetric and information-focused active measures against an opponent. As detailed by the US State Department in 1989 in reference to Soviet activities, "active measures" referred to a combination of disinformation and forgeries, front groups, non-ruling opposition parties, and political influence operations. Taken together, these were the basis for *maskirovka*, or the masking of warfare in the guise of harmless acts.[12]

As Bagge described the concept of reflexive control in the Russian strategy, "Reflexive control serves to undermine the very decision-making system itself, to make it favorable to the projector and thus to project power without committing significant military or political resources, nor meeting the acknowledged threshold of meddling in a sovereign's international affairs."[13] Reflexive control was a development of Soviet military doctrine that emphasized both disruption of the enemy's decision-making processes and feeding of disinformation in such a way that the enemy would react in a way advantageous to the Soviets/Russians. If an enemy commander perceived that his choices were limited to certain options, successful reflexive control would occur when those options played into Russian strategy, and the decision would be easier to anticipate.

Taken together, hybrid warfare, as understood by the Russian government and military, envisions a coherent strategy to undermine and destabilize an adversary, using a broad spectrum of means but (when possible) using an enemy's own weaknesses to play into the Russian strategy. The concept of reflexive control, after all, was to influence the information available to military officers, leading them into a predetermined (by the Russians) course of action that could be

[11] Maria Snegovaya, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare," Russia Report 1 (Washington DC: Institute for the Study of War, September 2015).

[12] Daniel P. Bagge, *Unmasking Maskirovka: Russia's Cyber Influence Operations* (Washington, DC: Defense Press, February 2019).

[13] Bagge, *Unmasking Maskirovka*.

planned for and which would play to Russian strengths in the battlespace. While difficult to realize fully in traditional warfare (although the British military and intelligence services have historically been more successful than many at strategic misdirection), with cyber technologies, the ability to achieve disinformation can be heightened. When successful, not only is the targeted society increasingly fragmented, but the targets themselves become messengers of disinformation and negative narratives.

Cognitive Hacking

Taking advantage of new and more widespread technologies, attackers are increasingly using psychological tricks and manipulations in the cognitive space. These tactics often mirror those used by hackers (phishing, spoofing, and others) and are a particular type of social engineering. Their use increases the possibility of gaining unauthorized access to information resources in cyberspace that are critical for the cognitive sphere of society, with the possibility of destructive effects on them. This phenomenon is called "cognitive hacking."[14] It is based on the manipulation of public consciousness performed in cyberspace – not only to steal money or data but also to influence the behavior of users, impose their will on them and control them. Almost any user of cyberspace can use cognitive hacking through disinformation campaigns and manipulation of reputation and/or distribution on Internet platforms of content that changes the perception of reality among other users. It can be carried out in the form of cyberattacks, cyber actions and operations aimed at manipulating the human perception of reality using the vulnerabilities of how people and social media process information. Such attacks aim to alter human behavior, perception, or attitude toward significant events or topics like the COVID-19 pandemic and are tailored toward a specific goal.[15]

In 2019 the volume of phishing attacks (the creation of fake sites or links that mimic the sites of well-known companies) grew by 400%. At the same time, more than 24% of malicious page addresses (URLs) were located on legitimate domains, relying on users' trust in them, and phishing became more personalized, including tracking the presence and activities of a particular user in cyberspace.[16] In addition to phishing, cybercriminals also use spoofing (disguising a

[14] Darren L. Linvill et al. "'The Russians Are Hacking My Brain!' Investigating Russia's Internet Research Agency Twitter Tactics During the 2016 United States Presidential Campaign," *Computers in Human Behavior* 99 (October 2019): 292-300, https://doi.org/10.1016/j.chb.2019.05.027.

[15] Ian Baxter, "The Cognitive Psychological Tricks Hackers Use to Dupe Users," *ITProPortal*, March 12, 2020, www.itproportal.com/features/the-cognitive-psychological-tricks-hackers-use-to-dupe-users.

[16] Muhammad Adil, Rahim Khan, and M. Ahmad Nawaz Ul Ghani, "Preventive Techniques of Phishing Attacks in Networks," in *Proceedings of the 3rd International Conference on Advancements in Computational Sciences*, ICACS 2020, Lahore, Pakistan, February 17-19, 2020 (IEEE, 2020), 1-8, ISBN 978-1-7281-4235-7.

malicious program as legal) as an in-road to political attacks. For example, in March 2016, one of the high-ranking officials of Hillary Clinton's campaign headquarters, John Podesta, entered his credentials on a page without recognizing a fake notification allegedly received from Google. After that, a hack occurred, and the attackers gained access to his data, which international and national political actors later exploited.[17]

Emotional Warfare

Along the murkier, non-kinetic spectrum of hybrid warfare, control of information targets not just cognitive processes but more limbic and emotional centers of the brain.[18] Humans naturally divide the world into various categories of identity as a way of making sense of a complex world and explaining why things happen as they do. Political psychologists have long demonstrated that these categories need not possess any intrinsic value. They can be completely arbitrary, constructed from myths, or handed down from authorities, whether by dividing schoolchildren into random groups according to eye color or national categories based upon historical events from centuries earlier. To outsiders, such divisions may appear arbitrary, such as Jonathan Swift's satire of differences between Catholics and Protestants in 1723. Still, inside social networks, such divisions can appear real and be reinforced by political, economic, and media practices.

Psychologists have identified trajectories along which ingroup/outgroup divisions can be turned from socially acceptable differences to potentially violent and intractable antagonisms. First, differences are essentialized or naturalized, meaning that broad stereotypes are placed on a group explaining that social differences (whether racial, linguistic, religious, etc.) are essential features of the group being described. When one is born into or raised in such a group, these differences are considered solidified and cannot easily be changed. The outgroup is then devalued according to these traits, with media images and stories often constructed to amplify these negative stereotypes.[19] These first two processes can often serve to help raise opinions of one's own group by highlighting differences in what makes one "good." American patriotism throughout the Cold War was often based on drawing the distinction between "hard-working Americans" and "inefficient, godless communists." In contrast, other nationalisms would

[17] Travis Farral, "Nation-state Attacks: Practical Defences against Advanced Adversaries," *Network Security* 2017, no. 9 (September 2017): 5-7, https://doi.org/10.1016/S1353-4858(17)30111-3.

[18] Linton Wells II, "Cognitive-Emotional Conflict: Adversary Will and Social Resilience," *Prism* 7, no. 2 (December 2017): 4-17, https://cco.ndu.edu/PRISM-7-2/Article/1401814/cognitive-emotional-conflict-adversary-will-and-social-resilience. We also credit Aleksandra Nesic for her work on emotional warfare.

[19] Marilynn B. Brewer, "The Psychology of Prejudice: Ingroup Love and Outgroup Hate?" *Journal of Social Issues* 55, no. 3 (Fall 1999): 429-444, https://doi.org/10.1111/0022-4537.00126.

strive to highlight the achievements of their own culture above others.[20]

The more dangerous progression is when the needs of communities are not or cannot be met, whether from basic needs, such as food becoming too expensive, to more existential threats of loss of culture or prestige. When such fears are present in a society, whether openly or latently, space opens for attribution of such threats to outsider groups. Historical anti-Semitism was often based on Jews being blamed for the financial troubles of the majority population, based upon stereotypes of their historical, social roles as bankers, lawyers, and academics. Dehumanization and/or depoliticization of groups, coupled with blame for a society's inability to reach basic goals or needs, draws upon perceived essential characteristics of a group to polarize opinion and accept violent remedies against the threatening outgroup.[21]

Propaganda campaigns during wartime have often employed such strategies, whether First World War stereotypes of German "Huns" killing innocent women and children, to US campaigns against the perceived fanaticism and inhuman nature of the Japanese.[22] The starkest examples, of course, occurred when the dehumanization of a group took on such proportions that genocidal violence was accepted and encouraged, whether against Jews in the Second World War, Muslims in Bosnia-Herzegovina, or "undesirables" in Khmer-Rouge era Cambodia.[23] Yet open warfare and a progression toward genocide need not be present for social divisions to be critical nodes in a conflict. The hybrid war model stops short of sweeping violence against a population in favor of using an adversary's divisions against itself.

US-know Thyself

The United States intelligence community has raised warnings about Russian interference in the American political system since at least 2016. The recent Mueller Report indicated that serious Russian efforts to influence elections date back to no later than 2014. Rather than being what some critics dismissively refer

[20] Robert T. Schatz, Ervin Staub, and Howard Lavine, "On the Varieties of National Attachment: Blind Versus Constructive Patriotism," *Political Psychology* 20, no. 1 (March 1999): 151-174, https://doi.org/10.1111/0162-895X.00140. It should be noted that some nationalisms are negative in nature, focusing on historical defeats and a sense of victimhood.

[21] Ervin Staub, "The Roots of Evil: Social Conditions, Culture, Personality, and Basic Human Needs," *Personality and Social Psychology Review* 3, no. 3 (1999): 179-192, https://doi.org/10.1207/s15327957pspr0303_2.

[22] Harold D. Lasswell, *Propaganda Technique in the World War* (Ravenio Books, November 2015).

[23] Michał Bilewicz and Johanna Ray Vollhardt, "Evil Transformations: Social-Psychological Processes Underlying Genocide and Mass Killing," *Social Psychology of Social Problems: The Intergroup Context*, ed. Agnieszka Golec de Zavala and Aleksandra Cichocka (New York, NY: Palgrave Macmillan, 2012): 280, https://doi.org/10.1007/978-1-137-27222-5_11.

to as "a few Facebook ads," the Russian efforts (both cyber and human) constituted a coordinated campaign to undermine trust in US institutions and increase political uncertainties and polarization.[24] That no definitive judgment has been made concerning precisely what effect such actions had on the 2016 elections is beside the point – if the goal was to increase uncertainty and undermine trust, even asking such questions has already accomplished a basic goal.

In many ways, the US was and remains a vulnerable target for cyber actions of hybrid warfare, even before the events of January 6, 2021. It is a country with deep political, economic, regional, racial, and gender differences. Most American political leaders have not emphasized the differences except along party lines, choosing instead to highlight common American political aspirations. Yet the latent differences and grievances remained available for exploitation, and cyber tools such as social media allowed unfettered access to millions of Americans. Led by the Russian GRU and IRA (Internet Research Agency), a directed campaign aimed to polarize Americans with such "wedge" issues as immigration, gender rights, and religion. A declassified US intelligence report from January 2017 summarized, "We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin, and the Russian Government developed a clear preference for President-elect Trump. We have high confidence in these judgments."[25]

The common perception was that, with Clinton as a front-runner in the election, Russian actions could help undermine her future presidency by sowing doubt as to its legitimacy. Cyber actions undertaken included infiltration of party (both Democratic and Republic) e-mail records, repackaging as cyber aggression selected communication via outlets like Wikileaks, creation of "astroturf" political groups on social media sites, sock-puppeting on sites like Facebook and Twitter to impersonate US voters, creation of fake protests and counter-protests, creation and dissemination of fake and misleading news reports, and much of this done through microtargeting selected populations in key states. The use of metadata from social media sites made this relatively easy, where users expressing keywords suggesting unease at immigration by Muslims, for example, could be fed ads and political messages to amplify such fears vis-à-vis certain candidates.[26]

---

[24] Robert S. Mueller, "Report on the Investigation into Russian Interference in the 2016 Presidential Election," The Final Report of the Special Counsel into Donald Trump, Russia, and Collusion (Washington, D.C.: US Department of Justice, March 2019), https://www.justice.gov/archives/sco/file/1373816/download.

[25] Bill Priestap, "Assessing Russian Activities and Intentions in Recent US Elections," Unclassified Intelligence Community Assessment (Office of the Director of National Intelligence, January 2017), p. ii.

[26] Philip N. Howard et al., "The IRA, Social Media and Political Polarization in the United States, 2012-2018" (University of Oxford, 2018).

While these Russian tactics were often successful, they could only find traction in a political landscape where significant divisions already existed, where fake news and conspiracy theories could take hold in a significant proportion of the population, and where technology had sufficient penetration – at least 30 million Americans were exposed to Russian messaging.[27] Rather than see themselves as Americans fighting in common against Russian operations, people in the US turned on each other along divisions of ingroup and outgroup, using language referring to "our" people, "real" Americans, and references to loyalty. Moreover, the IRA did not limit itself to electoral politics. It was also active in anti-science campaigns, notably in climate change and anti-vaccination circles. That this has helped in spreading otherwise dormant diseases such as measles (by spring 2019, some US states had declared states of emergency for the outbreaks) cannot be attributed solely to Russian activity but was meant to inflame undercurrents already present in American society[28] like cyber-surfing on existing topics that are "sensitive" to society or individual target groups.

The COVID-19 pandemic highlighted many of these differences, with divisions being exploited or created in response to public health responses. Protests against COVID vaccines in 2021 included both left- and right-wing groups, with the use of masks to prevent the spread of the coronavirus being associated along party lines.[29] Many actors were eager to fan such fires, disputing the virus's origins and its deadly nature, and such tropes were wrapped up in different disputes, more often politics than medicine. The larger strategy of both Russia and China was to cast doubt on the effectiveness of democratic institutions in response to the pandemic.[30]

The political psychology of ingroup/outgroup divisions helps explain how, when these divisions were reinforced through media and political narratives, the divisions became much starker both to outside observers and those who identified with one camp or another. This has not only made traditional bipartisan legislation and governing extremely difficult at the federal level, but the divisions have intensified. When new disinformation is spread (or biased targeted content triggers predetermined (planned) processes or perceptions), whatever the original source, Americans can share such information from person to person via so-

[27] Howard et al., "The IRA, Social Media and Political Polarization."

[28] David A. Broniatowski et al., "Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate," *American Journal of Public Health* 108, no. 10 (October 2018): 1378-1384, https://doi.org/10.2105/AJPH.2018.304567; Shanta Barley, "Climategate: Russian Secret Service Blamed for Hack," *New Scientist* 7 (2009).

[29] Rose Bernard, Gemma Bowsher, Richard Sullivan, and Fawzia Gibson-Fall, "Disinformation and Epidemics: Anticipating the Next Phase of Biowarfare," *Health Security* 19, no. 1 (2021): 3-12, https://doi.org/10.1089/hs.2020.0038.

[30] Sergey Sukhankin, "COVID-19 as a Tool of Information Confrontation: Russia's Approach," *The School of Public Policy Publications* 13, no. 3 (April 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3566689.

cial media, with selection algorithms (such as with Facebook) further strengthening the perception that such information can be trusted, because a trusted fellow American shared it. While Soviet propaganda in the 1970s and 80s had to work very deliberately to launder sources via multiple fronts, with cyber tools, a message or narrative can be released and spread with little effort, provided it reflects what people want or expect to see.

Social media techniques do not stand alone. Effective hybrid warfare uses various tools to achieve the aim of disruption or control. Attacks on energy infrastructure have also been documented in the US, with the US government admitting that denial-of-service attacks had disrupted grid operations in the Western United States in March 2019. Following knowledge that such attacks were possible and that breaches had previously been attempted, this opens the real possibility that the US could be hit with disruptions of critical services similar to what had previously been witnessed in Ukraine (which, in a sense, has become a testing ground for the technologies of future wars, in particular cyber, informational, and cognitive actions). The strategic goal of such threats or actions would be to create a feeling of uncertainty and insecurity, to keep both citizens and decision-makers off-center and anxious about how to interpret events and information.

Events in the US are admittedly of a much lower step of escalation than in other countries (i.e., Georgia, Estonia, Ukraine, Syria). Still, it is important to reiterate that there is no "red line" that distinguishes hybrid war strategies in one country versus another. The goals vary in the degree of destabilization desired, with some consideration for what might trigger an active response to the aggressor state. What the US experience has shown is that incremental and covert actions can weaken the response threshold over time, allowing greater interference and destabilization without a strong and coordinated defense.[31]

It's Warmer in the East

The continuing conflict in Ukraine is often cited as one of the primary examples of hybrid warfare in recent years, although many analyses refer primarily to the occupation of Crimea in 2014. The open conflict in regions of Donetsk and Luhansk since mid-2014 has received less attention and is often erroneously referred to in the western media as a "civil war." Even when analyses include discussion of violent conflict in the east, including the downing of Malaysian Airlines flight MH-17 in July 2014, these violent actions represent only the most visible aspects of the hybrid warfare spectrum.[32] This conflict has a number of specific

[31] Rubén Arcos, Manuel Gertrudix, Cristina Arribas, and Monica Cardarilli, "Responses to Digital Disinformation as Part of Hybrid Threats: A Systematic Review on the Effects of Disinformation and the Effectiveness of Fact-checking/Debunking," *Open Research Europe* 2, no. 8 (2022), https://doi.org/10.12688/openreseurope.14088.1.

[32] Irina Khaldarova and Mervi Pantti, "Fake News: The Narrative Battle over the Ukrainian Conflict," *Journalism Practice* 10, no. 7 (2016): 891-901, https://doi.org/10.1080/17512786.2016.1163237.

features, the most notable of which is the emerging evidence of non-kinetic (i.e., information warfare) having significant trauma impacts within society far from the front lines of eastern Ukraine.

Destructive actions focus on critical nodes in social and related systems, vulnerabilities that can be exploited, and then take on a self-sustaining, downward cycle of repeated steps and impacts (in scientific terms, positive feedback loops). Yet as the targeted nodes are dispersed across geographical and functional areas, it can be difficult for an outside observer to see the pattern of intended impacts and the overall strategy of the aggressor. It is vital for national security strategies to be able to identify and resist such dispersed and covert actions and to understand the complex and cascading impacts of aggressive actions that do not trigger the traditional concept of "acts of war."

As with other complex security systems, such as energy and environment, it is often not the initial impact that is most critical but the second and third-order effects that stem from the original disruption. Causal chains of events can be difficult to see at first, and inappropriate responses can worsen the chains of impact.[33] For instance, the Soviet government's response to the 1986 Chernobyl nuclear power disaster stands as perhaps one of the worst examples of a response. Then, political considerations led to the radiation exposure of tens of thousands of citizens in Ukraine and beyond. Similarly, inappropriate responses to changing conditions can easily worsen other disasters or conflicts.[34] Following precepts of reflexive control, an effective hybrid warfare campaign can lead a government into a positive feedback loop of worsening second and third-order impacts.

The hybrid war undertaken in Ukraine exhibits these strategic considerations of coordinated and planned actions and contains the necessary components in the cyber domain:

- Overall goals to be achieved
- Strategy for undertaking the campaign
- Organization of the campaign
- Tactics and instruments to be used
- Primary, secondary, and tertiary impact assessment
- Evaluation and reinforcement of consequences.

Cyber actions can be carried out sequentially, simultaneously, in parallel, and both in dispersed and focused manners. Dispersed-focused cyber actions aim at the infrastructure's most vulnerable elements (objects). A set of simultaneous and/or sequential cyber impacts provides synergistic effects on unpredictable

[33] Aura Reggiani, "Network Resilience for Transport Security: Some Methodological Considerations," *Transport Policy* 28, no. C (2013): 63-68, https://doi.org/10.1016/j.tranpol.2012.09.007.

[34] Andrew Leatherbarrow, *Chernobyl 01:23:40: The Incredible True Story of the World's Worst Nuclear Disaster* (Lancaster, UK: Andrew Leatherbarrow, 2016).

places (elements, systems, spheres) that may be administratively or politically separated from the initial target but functionally influence critical systems. As an example from the non-cyber world, in 2001, a series of anthrax attacks occurred on politicians via the US postal system, which was then forced to shut down mail rooms across Washington D.C. An unanticipated (for disaster planners) impact was that payment checks to the local utility PEPCO were not received, and the electrical utility had to approach the White House asking for funding, lest it cut off power to the US capital.[35] Cyber actions can have more immediate consequences in an even more interconnected world where companies rely on electronic payments and just-in-time deliveries of goods and components. For example, the June 2017 Petya cyberattacks on Ukraine had spillover effects into the European and global financial systems, even though the primary target was the Ukrainian state and domestic companies on the eve of the national holiday.[36]

While the 2017 Petya attacks met with an effective response from Ukrainian cyber forces, the intended targets of financial institutions quickly spilled over into hospitals and insurance companies around the globe. These methods work by designing cyber impacts with widespread chain effects. They disperse a destructive wave on interrelated objects and systems, simultaneously sparking impacts on multiple overlapping spheres. Cyberattacks can be implemented synchronously or asynchronously, in parallel along several lines of attack, or in serial multiple times on the same target cluster. Damage to the target objects is most destructive and effective according to the criteria of "efficiency-time-cost," although some targets may serve as a proof-of-concept to demonstrate capabilities to other potential target countries. A combination of research and combat analyses indicates that cyber-related actions and information warfare are increasing in scope and importance for warfighters.[37] In this context, hybrid warfare and its use of cyber assets are among the most important factors for understanding the future arc of conflict.

The December 2015 Russian cyberattack on the Prykarpattya Oblenergo power station required months of careful preparation and infiltration but disrupted electricity delivery for less than a day. It is possible that the real target of the attack was not just Ukraine. The attack might have been a test of new hybrid warfare techniques and a warning to other countries whose energy systems may be vulnerable to similar tactics. New cyberattacks in 2021 and early 2022 confirm

---

[35] Reshma Pradhan Lensing, "Historical Events and Supply Chain Disruption: Chemical, Biological, Radiological and Cyber Events," PhD Dissertation (Massachusetts Institute of Technology, 2003).

[36] Jagmeet S. Aidan, Harsh K. Verma, and Lalit K. Awasthi, "Comprehensive Survey on Petya Ransomware Attack," In *Proceedings of the 2017 International Conference on Next Generation Computing and Information Systems* (ICNGCIS), IEEE, pp. 122-125.

[37] Iskren Ivanov and Velizar Shalamanov, "NATO and Partner Countries Cooperation in Countering Asymmetric and Hybrid Threats in South Eastern Europe's Cyberspace," in *Toward Effective Cyber Defense in Accordance with the Rules of Law* 149, ed. Alan Brill, Kristina Misheva, and Metodi Hadji-Janev (2020): 59-70, https://doi.org/10.3233/NHSDP200041.

that a real information and cyber war is being waged on Ukraine, including the entire range of destructive impacts on both technical infrastructure and society. The use of social media to carry out cyberattacks is even more cost-effective, as they take advantage of the systems' own algorithms to spread disinformation or targeted narratives. Millions of people can be reached with relatively little effort, and when coupled with cyberattacks elsewhere (institutions, infrastructure), the social impacts can be sharply heightened.[38]

A Hybrid Form of Collective Trauma

The chaotic background of not knowing the future security risks in a country, how to interpret information or who to trust, and whether one can rely upon essential services or institutions, amplified by hybrid warfare, can lead to widespread states of cognitive resonance, dissonance, or imbalance. Beyond the confusion described by cognitive psychology, people can receive injuries measurable in terms of biological and neurological pathologies, where both individual and collective psychologies are pushed beyond normal perception, interpretation, and trust and fall into varying degrees of trauma.[39] Studies in Ukraine have measured the effects of trauma in zones near open conflict in the east. More recent research indicates that a more significant "hybrid war syndrome" may exist when the entire territory is a zone of active, destructive impacts upon individual and social psychologies.

The hybrid war consequences are not limited to the number of dead, maimed, and missing. They also include the effects on the cognitive sphere of citizens, communities, and society as a whole. Hybrid warfare, directly and indirectly, influences the conscious and subconscious, psychophysiological, mental state, and public health of conflict participants and bystanders. But in the cyber world of a hybrid conflict, witnesses do not only exist in the "hot zones" of kinetic warfare. Entire populations witness the conflict and are actively targeted by campaigns to undermine traditional concepts of identity, trust, and objective reality. In previous conflicts, trauma was experienced by those in a geographically defined war zone or where media could transmit disquieting images of war into people's living rooms. In contrast, cyber tools allow greater reach, erasing the older geospatial boundaries and one-way information flow. Both combatants and civilians, therefore, find themselves in the hybrid conflict zone, which manifests a number of psychological and behavioral characteristics that can be collectively labeled as "hybrid war syndrome" and its derivatives, "military-specific hybrid war syndrome," "specific PTSD of hybrid warfare," and others.[40]

---

[38] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid.

[39] Jack Saul, *Collective Trauma, Collective Healing: Promoting Community Resilience in the Aftermath of Disaster* 48 (Routledge, 2013).

[40] Yuriy Danyk and Oleksandra Zborovska, "Development and Implementation of a New Concept of Crisis Situations Syndrome: 'Syndrome of a Hybrid War'," *EUREKA: Health*

In countries experiencing protracted conflict, a stratum of people has developed a "military-specific hybrid war syndrome." This syndrome is attributed to the low, direct combat (military/kinetic) intensity of hybrid conflicts and the wide spectrum of unconventional parallel actions. Those experiencing heightened exposure to violence in a conflict zone often undergo substantial changes to individual psychology and reactions to the society around them, particularly when they return from the conflict zone and experience serious cognitive dissonance and dissociation.[41] Such individuals may have combat skills not applicable in civilian life and experience *hyperarousal* of threat perceptions (including potential aggression against imaginary threats), *intrusion* of traumatic memories on all aspects of life, and *constriction* in feeling that the traumatic experiences cannot be escaped. What differentiates this form from traditional combat trauma is that returning soldiers or participants do not return to a condition of peace or stability. Instead, they are still operating in an unstable environment in which threats and triggers permeate daily life.[42]

In many ways, the strategies of hybrid warfare not only create situations of direct trauma but mimic dissociative conditions for so long that psychobiological responses are indistinguishable. In describing combat trauma, Kardiner wrote, "…the whole apparatus for concerted, coordinated, and purposeful activity is smashed. The perceptions become inaccurate and pervaded with terror, the coordinative functions of judgment and discrimination fail… the sense organs may even cease to function."[43] In a hybrid war environment, an individual attempting to cope with constant stress and feelings of threat, hopelessness, and loss of control cannot easily rely on larger social reserves of resilience. When social trauma is experienced and groups begin to fragment, uncertainty and perceptions of risk are amplified by fellow members of society, a phenomenon greatly enhanced by accessing and using social media.

Those not experiencing combat or violence at the "front lines can still experience many of the stressors related to PTSD, and prolonged exposure to these influences has been shown to manifest as biophysiological markers in medical studies.[44] Though perhaps not surprising given hybrid war methods, it is remarkable that cyber tools allow penetration of acute stress into areas far removed

Sciences 6 (2018): 15-29, https://doi.org/10.21303/2504-5679.2018.00797; Piotr Pacek and Olaf Truszczyński, "Hybrid War and Its Psychological Consequences," *Torun International Studies* 1, no. 13 (2020): 23-30, https://doi.org/10.12775/TIS.2020.002.

41 Yuriy Danyk et al., "The Technology of Objective Diagnosis, Treatment and Prevention of PTSD in Members of the Armed Forces under Conditions of Hybrid War," *International Journal of Research and Innovation in Applied Science* 4, no. 1 (January 2019): 7-11, www.rsisinternational.org/journals/ijrias/DigitalLibrary/Vol.4&Issue1/07-11.pdf.

42 Judith L. Herman, *Trauma and Recovery: The Aftermath of Violence – From Domestic Abuse to Political Terror* (New York: Basic Books, July 2015).

43 As quoted in Herman, *Trauma and Recovery*, 35.

44 Iryna Boichuk et al., "Characteristics of Eye Movements in the Anti-terrorist Operation Area's Residents with Potential Posttraumatic Stress Disorder," *Journal of Opthamology* 1 (Ukraine) (2019): 52-55; Yuriy Danyk et al., "The Objectivization of the Complex

geographically from traditional conflict. These syndromes appear as a consequence of long-term, collective, and individual trauma from threats to life and health, to the constant change of form and intensity of combat tension, duration of combat and specific non-combat stress of varying intensity, all of which often exceed human capabilities for psychological resilience. The loss of comrades and participation in violence against the enemy are traditional triggers for PTSD. In hybrid campaigns like in Ukraine, effects are enhanced against a background of complex ethnonational identities. At the same time, the extent of outside stressors and their geographical scope pull social fabrics apart along targeted cleavages, leaving individuals with no firm idea of where they belong and what to believe in terms of current events and future goals. Called into question are ideas of a peaceful environment, standard values of society, and assessments by peaceful citizens of participants in hostilities.

In Ukraine, citizens must contend with competing narratives that the conflict in Donbas and Luhansk is the result of Russian incursion, a civil war between Ukrainians, the result of an ethnic division between Russians and Ukrainians, freedom fighters seeking independence from a corrupt Ukrainian government, or part of a larger expansion of power via "Novorossiya." The lack of a dominant narrative is intentional. The less agreement there is on the nature of the conflict, its causes, and how to assess those fighting it, the more stress and division can be caused within the non-combat areas of Ukraine and neighboring countries. In contrast to the strengthening of collective identities in the face of a clear aggressor (the American ideal of the Second World War), in a hybrid war, no one knows who the aggressor really is or why. Peace could come at any time or never, history becomes gaslit, and a sense of stability becomes ephemeral.[45]

The population's potential to protest against or support the conflict can also be used as an inroad for hybrid warfare exploitation in the target country. Frustrations and resentments borne from the larger conflict, coupled with perceptions of corruption or malfeasance among political, military, and business leaders, can easily be intensified by various cyber campaigns and targeting. The deterioration of the social and economic conditions and lack of opportunities to change lives for the better can be reflexively controlled to alter election outcomes or to spark migration from one region to another. Migrants can then be targeted as part of an ethnic or cultural "invasion" to alter political feelings in a third country. This phenomenon has been witnessed both within Ukraine in dealing with internally displaced people from Crimea/Donetsk/Luhansk, and then in stoking resentment against Ukrainians migrating to countries like Poland. Russian media disinformation campaigns have worked against Syrian refugees in

PTSD Diagnostic by Identifying Opthalmological Biomarkers," *International Journal of Research and Innovation in Applied Science* 4, no. 2 (January 2019): 7-11, www.rsis international.org/journals/ijrias/DigitalLibrary/Vol.4&Issue1/07-11.pdf.

[45] Joanna Szostek, "Nothing Is True? The Credibility of News and Conflicting Narratives during 'Information War' in Ukraine," *The International Journal of Press/Politics* 23, no. 1 (January 2018): 116-35, https://doi.org/10.1177/1940161217743258.

Germany and Latin American migrants in the United States by false stories planted and shared widely among domestic sources in Germany and the US.[46]

Cybersecurity Threats from the COVID-19 Pandemic in the Context of Hybrid Warfare and Cyber-Social Vulnerabilities

The COVID-19 pandemic is an acute test of the effectiveness of healthcare systems around the world and the capacity of state, local, and national governments to meet the relevant security challenges and threats. While the understandable focus of the coronavirus pandemic remains primarily on the direct health impact on populations and the response to economic effects, the outbreak has suddenly shifted societies' interactions based on information technologies. While cyber systems and information technologies may provide some positive opportunities, certain systemic security risks and vulnerabilities must also be identified and addressed from the perspective of hybrid warfare.

An immediate impact of the COVID-19 pandemic in China was not only to seal off cities from one another and a complete lockdown of the city of Wuhan, but the imposition of mandatory tracking apps on personal phones. South Korea sent texts detailing the movements of people suspected to be infected, raising serious privacy and accuracy concerns.[47] These tracking policies reflect technological capabilities and tracking movements in helping to predict the spread of infectious diseases like the coronavirus. Still, these were applied against the backdrop of concerns over homeland security, individual privacy, and potential exploitation by either government or nongovernment actors, especially with the regional and geopolitical transformations caused by the COVID-19 pandemic.

The European Commission announced its intention to track the movement of citizens through mobile technology in 2020. Thieri Breton, European Commissioner for Domestic Market and Services, assured that the EU plan did not have the goal of controlling people, and the data would remain anonymous and be deleted by the end of the pandemic. The European Data Protection Supervisor stated that this decision did not violate confidentiality rules. Vodafone, Deutsche Telekom, Orange, Telefonica, Telecom Italia, Telenor, Telia, and A1 Telekom Austria agreed to provide the data. In Germany, such surveillance was prohibited by law. Still, the COVID-19 pandemic opened a discussion about the need to intervene in the fundamental rights of citizens, especially by a state already imposing significant restrictions on freedom of movement. Jens Spahn, German Minister of Health, was the first to propose collecting data from the mobile phones of

[46] Stefan Meister, "The 'Lisa Case': Germany as a Target of Russian Disinformation," *NATO Review*, July 25, 2016, https://www.nato.int/docu/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm; Howard et al., "The IRA, Social Media and Political Polarization."

[47] Oleg Matyevchev, "What Did China Get in the Last Three Months, *LiveJournal*, March 20, 2020, accessed April 5, 2020, https://matveychev-oleg.livejournal.com/9896483.html. – in Russian.

infected individuals.[48]

Deutsche Telekom has already provided information on millions of its customers to the Robert Koch Institute (RKI). RKI specialized in the study of infectious diseases and was central in discussions about information policy concerning the COVID-19 pandemic. Virologists at RKI hoped to construct maps of the movements and German residents and understand how long people in urban environments were exposed during the pandemic lockdown. All such information made it possible to predict infectious disease spread more accurately; it also allowed building a system for quickly calculating all the social connections of a given individual: who the person was in contact with, who was traveling with the person, where he/she was, and with whom they spoke.[49] For example, such mass surveillance systems have been introduced in countries such as China and Russia. In Russia, Prime Minister Mikhail Mishustin proposed systems to track all individuals suspected of being infected with COVID-19 by geolocation of their mobile phones. Many countries have also proposed new surveillance programs to better plan for hospital needs and available resources. However, this required a significant relaxation of medical data confidentiality and demonstrated a blurring of the lines between privacy, the public good, and whether the institutions that hold such information can be trusted.[50]

Trust, Fakes, and Disinformation

The issue of trust moves beyond that of individual governments. In disaster situations, verifiable information is always a valuable commodity, and in prolonged stress situations, people become more vulnerable to innuendo, rumor, and deliberate disinformation. The ease of such disinformation spreading across the globe is greatly amplified by modern information networks, from instant communication apps to social media. The COVID-19 pandemic has created fertile ground for developing and spreading conspiracy theories. Where information is lacking, and uncertainty is high, this vacuum is easily filled with disinformation and unverifiable stories.[51] The coronavirus presents particular problems concerning disinformation: the long incubation period, the fact it can be spread by asymptomatic people, the international origins of the virus, combined with the

---

[48] Foo Yun Chee, "Vodafone, Deutsche Telekom, 6 Other Telcos to Help EU Track Virus," *Reuters*, Technology News, March 25, 2020, accessed April 1, 2020, https://uk.reuters.com/article/us-health-coronavirus-telecoms-eu/vodafone-deutsche-telekom-6-other-telcos-to-help-eu-track-virus-idUKKBN21C36G.

[49] "Geolocation Surveillance: What Is Allowed in Germany for the Fight Against Coronavirus," *DW Made for Minds Journal*, April 2020.

[50] Radu Mîrza, "COVID-19 and Digital Rights in Romania, Moldova and Ukraine," *Central and Eastern European EDem and EGov Days* 341 (March 2022): 195-211, https://doi.org/10.24989/ocg.v341.14.

[51] Sally McManus, Joanna D'Ardenne, and Simon Wessely, "Covid Conspiracies: Misleading Evidence Can Be More Damaging Than no Evidence at All," *Psychological Medicine*, no. 1-2 (2020), https://doi.org/10.1017/S0033291720002184.

public health policy dilemma of proving a negative. Model projections of potential deaths can be altered by significant social distancing, and the original warning estimates can be overstated. Economic costs are more obvious and immediate, while public health benefits are largely ephemeral until lost.[52]

One of the main conspiracies associated with the coronavirus was that it is of artificial and deliberate origin, created in the laboratory of some country. The 2019 dispute over China's researcher at the National Microbiology Lab in Winnipeg served as a basis for false claims that the Canadian government had created the virus, which was then stolen and released by a Chinese researcher.[53] Canadian disputes with the Chinese telecom company Huawei also became part of conspiracy theories, asserting that 5G networks are responsible for the spread of the virus. Picked up in Britain, the 5G conspiracy has resulted in attacks on numerous cell phone network towers.[54] In many countries during 2020-2022, a variety of information about the pandemic was disseminated, both with significant inaccuracies and mis/disinformation.[55] This often-controversial information has been featured in many official briefings and news networks, covering almost every aspect of COVID-19.[56]

Conflicting messages in public policy responses, information, and media commentary in virtually every country have created considerable confusion about the extent of the risks associated with the pandemic, with sharp divisions over the danger from the virus. Some theories have centered on how some figures have used the media to conspire to undermine the authority of certain politicians or medical experts and that claims of potential infection and death from COVID-19 have been greatly exaggerated. Such patterns of disinformation in Ukraine have caused more than just stress and uncertainty. Thus, one should recall the violent protests in Ukraine that broke out in February 2020 based on false information about the risks of the spread of the virus by citizens returning from China. Social media disinformation about the pandemic circulated in Ukraine throughout 2020-2021 and significantly hampered government efforts.

The disinformation messages are therefore tailored to amplify uncertainty and sow doubt. Texts and messages are often presented in a trusting manner,

---

[52] Edward Lucas, "Mutations of Misinformation," *Tyzhden.ua*, March 1, 2020, accessed 5 April 2020, https://tyzhden.ua/Columns/50/240946.

[53] Dax Gerts et al., "'Thought I'd Share First' and Other Conspiracy Theory Tweets from the COVID-19 Infodemic: Exploratory Study," *JMIR Public Health and Surveillance* 7, no. 4 (April 2021): e26527, https://doi.org/10.2196/26527.

[54] Takele T. Desta and Tewodros Mulugeta, "Living with COVID-19-Triggered Pseudoscience and Conspiracies," *International Journal of Public Health* 65, no. 6 (2020): 713-714, https://doi.org/10.1007/s00038-020-01412-4.

[55] Sahil Loomba et al., "Measuring the Impact of COVID-19 Vaccine Misinformation on Vaccination Intent in the UK and USA," *Nature Human Behaviour* 5, no. 3 (2021): 337-348, https://doi.org/10.1038/s41562-021-01056-1.

[56] Emily Chen et al., "COVID-19 Misinformation and the 2020 U.S. Presidential Election," *Harvard Kennedy School (HKS) Misinformation Review*, March 3, 2021, https://doi.org/10.37016/mr-2020-57.

with an address to a close personal acquaintance. They usually contain all the information about something that may excite the recipient but also include a call to action. Individuals are told what to do to protect themselves; they are also asked to spread this "secret" invaluable information to help as many other people as possible. Often the motive behind such reports is the assertion that authorities are hiding either solutions to the pandemic or its sources. The source of this information is generally not specified and is usually included in the narrative as an expert and acquaintance. The sources of information may either be foreign, intending to create disorder, or maybe domestic actors with a financial interest in spreading disinformation. PRC disinformation efforts visibly shifted in 2020 to target individual phone text users in the US, specifically to spread COVID-related disinformation.[57]

Disinformation campaigns have long-term consequences not only directly to individuals who may take harmful actions but are also damaging the social and political fabric in environments where verifiable and false information cannot be distinguished. Information technology in the decentralization of news sources makes the rapid dissemination of false information nearly uncontrollable and very difficult to overcome. After the Chernobyl incident in 1986 in Ukraine, it was often said that hundreds were killed by radiation and many thousands by information. In a pandemic, it is difficult to quantify the number of casualties associated with inaccurate information, mis- or disinformation, but conservative estimates indicate that thousands of lives could have been saved with more timely government intervention and public health action.[58]

Such intense cyber informative influences cause a stressful state for many people, which is maintained for a long time with varying intensity. This condition can be described as "pandemic information stress," which in the future may be exposed to various psychosomatic changes: post-traumatic stress disorders (PTSD), the development of anxiety-depressive states, panic attacks, the formation of phobias, and obsessive-compulsive disorders consequences. Their emergence and evolution are significantly influenced by the state of the economy, the threat of lowering living standards, unemployment, and insecurity in the future.[59] The global trend has become a replication of false information on social networks, the distribution of photos and videos without a clear context

[57] Edward Wong, Matthew Rosenberg, and Julian E. Barnes, "Chinese Operatives Helped Sow Panic in U.S., Officials Say," *The New York Times*, April 23, 2020, A10.

[58] Nicholas Charron, Victor Lapuente, and Andrés Rodriguez-Pose, "Uncooperative Society, Uncooperative Politics or Both? How Trust, Polarization and Populism Explain Excess Mortality for COVID-19 across European Regions," The QoG Institute Working Paper 12 (Göteborg, Sweden: The Quality of Government Institute, Department of Political Science, University of Gothenburg, December 2020), http://hdl.handle.net/2077/67189.

[59] Ali Farooq, Samuli Laato, and AKM Najmul Islam, "Impact of Online Information on Self-Isolation Intention during the COVID-19 Pandemic: Cross-Sectional Study," *Journal of Medical Internet Research* 22, no. 5 (2020): e19128, https://doi.org/10.2196/19128.

but with a clear emotional focus, the reliability of which is difficult to assess at the time of viewing. During a pandemic, such informational effects have particularly severe social consequences and become a powerful tool of hybrid warfare.

Cyber Crimes and Espionage

A related yet distinct issue is the intensification of cybercrime. Some crimes are directly related to medical institutions and their information systems. For example, criminals are looking for information about drugs, tests, or vaccines related to coronavirus for sale on the black market. Another trend is the circulation of counterfeit so-called coronavirus drugs and the open market, considering everyone's familiarity with the virus and intense desire to avoid infection. In addition, destructive cyber actions aim at violating medical institutions' health facilities and stealing confidential data. Some attempts also include the encryption of large volumes of critical medical data to obtain ransom for their restoration. The pandemic has opened hospitals, research centers, and universities to attacks by organized cyber criminals. Attacks were carried out against the University Hospital in Brno, Czech Republic, a major COVID-19 testing center, the British Hammersmith Medicines Research, which develops COVID-19 vaccines, AP-HP Paris Hospital, and a number of Spanish hospitals. In addition, the World Health Organization (WHO) warned of suspicious e-mails received from attackers trying to take advantage of the emergency to steal money and confidential information, as well as attempts to hack into WHO's computer systems and its coronavirus database.[60] European Commission President Ursula von der Leyen has warned that cybercrime in the EU has increased due to the coronavirus outbreak. "They follow us on the Internet and use our fears about the coronavirus. Our fear is becoming their business opportunity," EU Observer reported.[61]

The sudden shift to remote working and banking also exposes many people to theft through financial systems or commercial and industrial networks that were never intended to be widely distributed. One fear among cyber security experts has been that businesses will take shortcuts in their network security in order to maintain profits during the severe economic downturn. Commercial and industrial information will be shared across private networks and on personal computers, with IT security unable to police the use of these open networks. For countries already at risk for acts of industrial espionage before the pandemic, cybercriminals and outside actors will not fail to see the opportunities available to them.[62]

---

[60] World Health Organization, "Beware of Criminals Pretending to be WHO," April 2020, accessed April 5, 2020, https://www.who.int/about/cyber-security.

[61] "The EU Recorded a Sharp Increase of Cybercrime: What Is Happening," *Informacionnoe Soprotivlenie*, March 25, 2020, accessed April 1, 2020, https://sprotyv.info/analitica/v-es-zafiksirovali-rezkij-rost-kiberprestupnosti-chto-proishodit.

[62] Eduard Babulak, James C. Hyatt, Kim Kyu Seok, and Jang Sun Ju, "COVID-19 & Cyber Security Challenges US, Canada & Korea," *Transactions on Machine Learning and Data*

Education and Transition to E-Learning

Education is another critical issue directly related to the pandemic and cyber-social vulnerabilities in hybrid warfare conditions. Due to COVID-related quarantines, there were crucial changes in the established rhythms of life, work, and study of all segments of the population in almost all countries. For the first time, humanity faced a pandemic of this level in the context of a high-tech information society, globalization, and easily accessible global travel. Business, tourism, migration activity, and population mobility were disrupted overnight. The forced, real, rapid, and massive transition to e-learning in all spheres and at all levels of education became stressful for all participants of the educational process, who were forced to master new tools and methods hastily.

Education under pandemic conditions has become a strategic issue with far-reaching implications for the whole world. UN Secretary-General António Guterres noted that about one billion students and schoolchildren in 160 countries worldwide could not receive full education due to the closure of educational institutions caused by the coronavirus epidemic. It threatens the world with a "generational catastrophe." According to polls conducted in Ukraine in July 2020 and estimates by the State Service for the Quality of Education of Ukraine, e-learning in schools is not supported by 48% of parents and 45% of students, whereas only 9.9% of the respondents "fully support" e-learning.[63]

The problems lie not only in the essence of e-learning but also in the socio-technical contradictions and cyber-social vulnerabilities associated with it. E-learning is multifaceted and multidisciplinary. The issue includes technical, social, demographic, psychological, content-informational, methodological, didactic, organizational, cyber, and other aspects, as well as the ability of governments to train personnel for developing and delivering e-learning. The students must be prepared for the correct and effective use of technologies while protecting their mental and physical health in uncertain and stressful conditions.

Educational issues that have arisen in the context of hybrid confrontation and pandemic directly affect all spheres of state functioning and areas of national security. In general, this is a question of the fate of the state and the statehood of their further existence and development. In the absence of government control and regulation, e-learning can potentially lead not only to an increase in inequality in education and the loss of human potential but also to perilous changes in information processing, critical thinking, and social media dependence that may leave them vulnerable to cognitive and emotional cyber warfare techniques.

Mining 13, no. 1 (2020): 43-59, http://www.ibai-publishing.org/journal/issue_mldm/2020_October/13_2_43_59_mldm.pdf.

[63] Yuriy Danyk and Tamara Maliarchuk,"Strategic Aspects and Problems of E-learning in the Context of Pandemic and National Security," *S-Direct 24* 3, no. 14 (July 2020), International scientific journal published under the auspices of NATO Defence Education Enhancement Program.

The pandemic has generated a demand for official e-learning standards for training specialists and the development of e-learning courses, which will help evaluate the e-learning processes' effectiveness and promote the systemic approach in a new mode of education in countries from the United States to Ukraine. It means that e-learning requires standardization, systematization, and strategic approaches to ensuring effective remote education while providing resources to deliver aims on a tactical institutional level. Even though the pandemic will end sooner or later, education (civil, government, and military) is unlikely to return to its former normalcy, and the implications for national security must be considered. COVID-19 has forced enormous and sudden changes upon societies, and our dependence upon technology requires intelligent public policy decisions concerning not only response to the virus itself but recognizing the vulnerabilities that technologies introduce.

Conclusion

This article aimed to outline the main problems caused by hybrid warfare, COVID-19, and possible solutions in cyberspace, social life, and national security that impact all spheres of state functioning. Exploiting cyber-social vulnerabilities plays a special and increasing role in hybrid conflicts. The creation of effective national cybersecurity and cyber defense system of the state, including the characteristics of cyber-social vulnerabilities, is one of the most important priorities in ensuring national security and defense. Effective early warning of cyber-social vulnerabilities requires structural and parametric analysis of cyber systems and their users and an understanding of how messages propagate, are received, and reproduced in cyber ecosystems. Strategies for increasing the resilience of information systems rely not only on "citadel" models of keeping intruders out but how to prepare populations for tricks, hacks, and disinformation campaigns from within and external agents.

The primary strategic aims of hybrid warfare tend to be destabilizing – that is, not the physical occupation of territory but sowing distrust in institutions and information itself. Such attacks have a destructive impact not only on critical infrastructure but also on society. It was established that the main destructive cyber actions were carried out selectively and focused on vulnerable cyber-social elements. The use of destructive focused cyberattacks was carried out as a part of large-scale complex cyber operations.

The main problems arising or manifested in connection with the COVID-19 pandemic in the context of hybrid warfare are as follows:

- Insufficient readiness of cyber-social health care systems of most countries;
- Significant restructuring of major national economic processes as a result of COVID-19 responses and the formation of new models of life and society;

- Rapid and complete immersion of the population in cyberspace and the transition to remote, distant modes of work and study;
- Growth of activity in social networks, increase in volumes of online trade, streaming entertainment, and online services (e.g., telemedicine, e-learning, e-banking);
- An increase in a wide range of cybercrimes, the spread of fake news related to the pandemics, misinformation, and information oversaturation of society;
- Insufficient level of cyber information literacy, inability or unwillingness to use Internet systems and IT technologies in everyday life, and failure to ensure cyber and information security, especially in the context of the global hybrid war.

While we have previously discussed developments in cyber-hybrid warfare, the COVID-19 pandemic has accelerated both activities and vulnerabilities associated with privacy, isolation, shifting identities, and propagation of disinformation.[64] The pandemic has allowed the further intrusion of destabilizing actors into people's lives, higher dependence on virtual information as traditional social ties have been disrupted, and further reliance on cyber technologies for all aspects of life.

The introduction of control over the implementation of quarantine requirements with the use of high-tech means deserves special attention. Failure to take precautionary measures to protect the rights of citizens in a timely manner is likely to violate the confidentiality of personal information. There is reason to predict that such control and supervision of citizens and their activities in many countries, especially with authoritarian regimes, may not only remain but even intensify once the pandemic subsides. Such a progression poses a threat to one's home country and provides inroads for outside actors to exploit and leverage such "social credit" systems to their benefit. The more dependent we become on such technologies, the more vulnerabilities allow the exploitation of such linkages, now largely independent of traditional social resilience. What are the security implications of cases when outsiders change medical records, place people on "no-fly" lists, or spoof their identity not only for loan applications but in worldwide media?

The COVID-19 pandemic has shocked the global system, not only in terms of economic activity and cross-border travel, but in how we relate to technology, how we measure and value social and political resilience, and our abilities to respond to the spectrum of hybrid warfare attacks that exploit cyber technologies and vulnerabilities. Our societies become ever more vulnerable to cognitive and emotive warfare that overwhelms our information processing, bypasses rational

[64] Tamara Maliarchuk, Yuriy Danyk, and Chad Briggs, "Hybrid Warfare and Cyber Effects in Energy Infrastructure," *Connections: The Quarterly Journal* 18, no. 1-2 (2019): 93-110, https://doi.org/10.11610/Connections.18.1-2.06.

thought, and hits us at a basic "survival" level, often as part of a strategy to further divide our societies and put institutions into question. While we have long expected cyber-hybrid warfare to become more important, it is now critical to address deficiencies in disinformation, privacy, cybercrime, and e-learning, all of which can affect larger questions of security and stability.

Thus, the research promoted the definition of Cyber War or Cyber Conflict in cyberspace and (or) through cyberspace. The confrontation in cyberspace and (or) through cyberspace is a complex socio-political phenomenon employing cyber intelligence, cyber defense, and cyber weapons for causing various losses to the enemy in different fields and minimizing own losses in economic, military, political, social, cyber, information, ideological, and other spheres. Unlike other destructive influences, conflicts, and (or) wars, cyber warfare (cyber conflict, destructive cyber actions) is not proclaimed. And if it begins, it does not end, being conducted continuously until one of the parties of the conflict is completely defeated or unable to continue the destructive actions. It can be completed only in case of the destruction of cyberspace.

While military strategies remain in place, the soft underbelly of society is increasingly under assault.

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. 20, 2021, is supported by the United States government.

About the Authors

Dr. **Chad Briggs** is an Associate Professor and Director of Public Policy and Administration at the University of Alaska Anchorage. Dr. Briggs has field experience in information and hybrid warfare and in developing defensive strategies to protect critical systems in Eastern Europe and the Balkans. He has a Ph.D. in political science from Carleton University in Canada. He has been previously a senior advisor for the US Department of Energy and the Minerva Chair and Professor of Energy and Environmental Security for the US Air University (USAF). He is the author (with Miriam Matejova) of *Disaster Security: Using Intelligence and Military Planning for Energy and Environmental Risks*.
E-mail: chad.briggs@alaska.edu

Major General **Yuriy Danyk**, Professor, Doctor of Engineering Sciences, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute." Dr. Danyk is an expert in the art of war, national defense and security, information and cybersecurity, electronic and IT technologies, the design and application of robotic complexes, and special forces development. He has combat experience in the application of advanced defense technologies in the conditions of modern war.
E-mail: zhvinau@ukr.net

Dr. **Tamara Maliarchuk** was a member of the NATO working group on DEEP program implementation in the Armed Forces of Ukraine. She was an analyst with the S. Korolov Zhytomyr Military Institute in Ukraine and has worked with US forces on language and cyber defense. She conducts research in e-learning, innovative technologies in PTSD detection and therapy, and manipulative technologies in the web environment.
E-mail: maliarchuktamara@gmail.com