Information & Security: An International Journal

Carol Atkinson, v.39:1, 2018, 63-76 https://doi.org/10.11610/isij.3906

HYBRID WARFARE AND SOCIETAL RESILIENCE: IMPLICATIONS FOR DEMOCRATIC GOVERNANCE

Carol ATKINSON

Abstract: This article examines the changing nature of warfare and the implications for democratic governance. The first section describes "hybrid warfare" – the central concept used by NATO to characterize modern war. It looks at the evolution of the concept, how it is defined, and some disputes over its ability to accurately capture the essence of modern war. In NATO, the concept of "hybrid warfare" is used to analyze and characterize Russian actions in Ukraine and Crimea; however, the Russian military thinks a bit differently about modern warfare and does not use the term to characterize its own actions. Thus, in the second section, the article examines the difference in Russian military thinking from that of the West. One of the main differences is the role and nature of cyber operations. Cyber operations, especially influence campaigns that include propaganda, disinformation, and "winning hearts and minds," are key 'irregular' components of hybrid warfare that seek decision through influencing the beliefs, values, and collective identity of the opponent's population. Finally, in its third section, the article argues that the ability of any democratic country to counter hybrid threats, in large part, depends on the willingness of its citizens to support government policies that ultimately undermine the basic freedoms that define what it means to be a democratic country. The author suggests that democratic governance is being undermined by the policies that democratic countries, with the support of their citizens, institute in order to combat hybrid threats, particularly cyber threats.

Keywords: hybrid warfare, hybrid threats, surveillance, democratic governance.

Hybrid Threats, Hybrid Warfare

The concept of "hybrid warfare" entered Western security discourse in the early 21st Century. It characterizes and categorizes aspects of modern warfare that needed to be better addressed and emphasized in national security strategies. For example, there were emerging threats that did not fit well into conventional ideas on the use of armed force. These included the increasingly important, sometimes decisive, role played by superpowered individuals,[1] cyber hackers/attackers, and social media activists/ exploiters. Such non-state agents were able to achieve significant political objectives in-

cluding the overthrow of governments in the Arab Spring protests, the Egyptian Revolution, and the territorial expansion of ISIS/Daesh. Cyber operations were also used to achieve strategic military objectives such as the physical destruction of Iranian uranium enrichment centrifuges. "Hybrid warfare" simultaneously describes a world that has become "flatter" as information and communication technologies are widely available and variously "peaked" as individuals who so desire have easier access to destructive technologies and the ability to use them to influence policy.

One of the earliest writers to use the term "hybrid warfare" was Frank Hoffman who traced its lineage to Robert G. Walker's Naval Post Graduate School thesis of December 1998 in which Walker characterized "the Marine Expeditionary Unit as 'a hybrid force for Hybrid Wars'."[2] Doctrinally, hybrid warfare strategies are those that combine conventional and unconventional methods to achieve objectives. The idea is not revolutionary, but evolved from conceptualizations of modern warfare from scholars such as John Mueller who in the early 21st Century argued for two conceptualizations of warfare: tradition warfare and criminal warfare. The first matching our 20th Century concept of warfare as disciplined military forces used as instruments of the state where opposing armies meeting on a geographically bounded battlefield to determine which state's policies will prevail. The second, criminal warfare, matching some of the characteristics mentioned above where a variety of non-state entities (organized criminal groups, terrorist groups, pirates) use unconventional methods to obtain their own objectives.[3] However, there are significant differences between Mueller's conceptualization and hybrid warfare.

First, in hybrid warfare regular and irregular forces are not seen as separate military tools to be pulled out for use as the strategic situation might dictate; rather they are used synergistically as an all pervasive tool of government influence, not necessarily a tool of military strategy. Second, in hybrid warfare regular military forces may or may not be the final arbitrator of victory. Irregular forces are used to achieve decisive results, and can prevail over militarily superior opponents by making military action difficult to implement or even superfluous. "These forces," Hoffman argued, "become blurred into the same force in the same battlespace. While they are operationally integrated and tactically fused, the irregular component of the force attempts to become operationally decisive rather than just protract the conflict, provoke overreactions or extend the costs of security for the defender."[4] In hybrid warfare, the ideal situation is one in which irregular components can be used decisively to achieve strategic goals without the need to resort to the use of regular military forces.

The concept of "hybrid warfare" found additional traction in the early 21st Century when the North Atlantic Treaty Organization (NATO) picked it up. In 2011 the NATO multinational exercise called "Countering Hybrid Threats" was used to test concepts in NATO's new 2010 Strategic Concept. According to Michael Aaronson,

General Yves de Kermabon, General Sverre Diesen, and Mary Beth Long of NATO's Allied Command Transformation, "The new threat confronting NATO's diverse nations is insidious and not easily defined or identified. It flourishes in the seams between states, and in the soft areas of bad or weak governance. The new threat consists of distinct but tangled elements; hence the rubric "Hybrid Threat."[5]

Through the use of the term "hybrid warfare," NATO sought to incorporate the role played by irregular agents such as terrorists, information technologists, citizen activists, and the use of asymmetric strategies into mainstream strategic thought and military operational planning. NATO used the term "hybrid warfare" to characterize Russian operations in Ukraine and Russian strategies used to annex Crimea in 2014. The Russian strategy in Ukraine included traditional military tactics as well as irregular forces such as masked troops without state insignia and Russian sponsored non-state agents such as motorcycle gangs as well as cyber attacks and disinformation campaigns. As seen in the Ukrainian case, these irregular components were difficult to counter, particularly with NATO conventional armed forces and operational concepts.

The concept of "hybrid warfare" and its usefulness is disputed. Damien Van Puyvelde writing in *NATO Review* argued that "Rather than develop strategies based on 'hybrid' challenges (an elusive and catch-all term), I believe decision-makers should stay away from it and consider warfare for what it has always been: a complex set of interconnected threats and forceful means waged to further political motives."[6] Interestingly, hybrid warfare is not included in the U.S. Department of Defense Dictionary of Military and Associated Terms in the current 15 October 2016 edition.[7] Although NATO applies the concept to characterize Russian military strategies, the Russian military itself does not use the concept to describe its own ideas on warfare, but uses the term "indirect and asymmetric methods."[8] In his analysis of Russian strategic thought Charles Bartles of the U.S. Army's Foreign Military Studies Office argued that hybrid warfare was a Western conceptualization and did not encompass Russian military thinking about the nature and content of modern warfare. The Russian term "indirect and asymmetric methods" encompassed a broader strategic vision and implied the use of all instruments of national power. From the Russian perspective:

> War is now conducted by a roughly 4:1 ratio of nonmilitary and military measures. These nonmilitary measures include economic sanctions, disruption of diplomatic ties, and political and diplomatic pressure. The important point is that while the West considers these nonmilitary measures as ways of avoiding war, Russia considers these measures as war.[9]

While the usefulness of the term is disputed, nevertheless discussions on hybrid warfare have highlighted the necessity to consider how various "irregular" agents and in-

struments are used and the military and political implications of their use. At the forefront of these discussions is cyber; the use of new and emerging communication, information, and computing technologies.

Cyber: The Information, Communication, and Computer Component

The use of information and communication technologies to support military forces in the conduct of military operations is nothing new; spies, reconnaissance, surveillance, and intelligence analyses have always played a role in military campaigns. Additionally, militaries around the world and throughout time have always sought to incorporate the newest technologies into their armies and navies. What is revolutionary in the 21st Century is the pervasiveness of new cyber technologies in every aspect of modern life. They are used to communicate and disseminate information; to collect intelligence and conduct surveillance; and, to store and analyze huge amounts of data. The Internet of Things consisting of interconnected "smart" devices such as cell phones with embedded micro-computers in cars, homes, offices, and everyday electronics; with sensors, satellites, and surveillance cameras; with electrical power grids, and so on is unprecedented. Also revolutionary is the use of computer networks to connect ordinary people with each other instantaneously and across great distances. Cyber technologies give each person the ability to create, disparage, support, and disseminate information and shape beliefs, values, "facts," and other ideas through individual and personal channels of information (such as Twitter, Facebook, etc.).

In some respects, there is a lot that is new in modern warfare. As just described, emerging communication and information technologies have given a wide range of ordinary people (with the requisite computer skills) the ability to do a number of things that were previously centralized in government organizations or corporate headquarters: cyber espionage, control of industrial networks through cyber systems; covert networking of like-minded individuals; access to sensitive information including weapons technologies (IEDs for example); conduct of large-scale propaganda/disinformation campaigns; access to personal communications between world leaders; access to personal data (emails, addresses, social connections, financial status, etc.) on anyone whether connected to the worldwide web or not; and the list goes on. The technologies can be used to obtain policy changes through blackmail, control of processes and systems, and most insidious: through the ability to shape the facts, news reporting, values, beliefs, information, and other ideas of an opponent in order to influence the actions, military or otherwise, that the opponent is capable or willing to take.

The pervasiveness of networked and embedded computers in our lives is also the genesis for the strategy shift that we see reflected in hybrid warfare. All of these phenomena that are associated with computing and information technologies present a

new paradigm for state policy. In many ways, they move the struggle for power in the international system away from military and political strategies that focus on the use of material capabilities (armed attack, military deterrence, economic sanctions, embargoes, and the like) toward the control and dissemination of information for use in shaping and, ultimately, controlling ideas and, hence, actions.

In other respects, these aspects of modern warfare are not so new, but a return to ancient military and political ideas and strategies. The modern ability to gather, organize, analyze, and use vast amounts of data provides the means to more effectively apply the core strategic ideas encapsulated in Sun Tzu's *The Art of War* from the 4th Century BC. This ancient strategic manual described the use of an indirect approach to achieving strategic objectives through deception, the creation of false appearances, fomenting internal discord and nurturing subversion and distrust. Modern technologies simply provide more interesting and, perhaps more effective, ways to implement these strategic ideas. In this sense, modern information, computing, and communication technologies provide increased capability for both state and non-state agents to achieve one of the oldest of strategic goals: to "subdue the enemy without fighting" by "attacking the enemy's strategy."[10] Russian analysts Sergey G. Chekinov and Sergey A. Bogdanov described Russian New-Generation Warfare in much these same terms: "In its new technological format, the indirect action strategy will draw on, above all, a great variety of forms and methods of nonmilitary techniques and nonmilitary measures, including information warfare to neutralize adversary actions without resorting to weapons (through indirect actions), by exercising information superiority, in the first place."[11]

Russia's use of cyber operations, espionage, disinformation, and news media to undermine trust in international and domestic institutions is cited in the West as the quintessential example of the use of the cyber component in hybrid warfare. Yet, the Russians would point to how the United States has used these same mechanisms to promote its democratizing agenda. From the Russian perspective, the United States used nonmilitary measures such as arms sales, special operations forces, private military companies, nongovernmental organizations, protestors, activists, and "constant information warfare" to further its political goal to spread democratic governance.[12] As examples, Russian military scholars point to the United States' efforts to institute regime change in Iraq, Afghanistan and countries of the Arab Spring where mass media, the internet, social media, and nonstate agents were used to foment dissent in order to create a political and social environment more susceptible to overthrow using conventional military operations.[13] Bartles described the Russian perspective:

> Russia believes that the pattern of forced U.S.-sponsored regime change has been largely supplanted by a new method. Instead of an overt military invasion, the first volleys of a U.S. attack come from the installment of a political

> opposition through state propaganda (e.g., CNN, BBC), the Internet and social media, and nongovernmental organizations (NGOs). After successfully instilling political dissent, separatism, and/or social strife, the legitimate government has increasing difficulty maintaining order. As the security situation deteriorates, separatist movements can be stoked and strengthened, and undeclared special operations, conventional, and private military forces (defense contractors) can be introduced to battle the government and cause further havoc. Once the legitimate government is forced to use increasingly aggressive methods to maintain order, the United States gains a pretext for the imposition of economic and political sanctions, and sometimes even military sanctions such as no-fly zones, to tie the hands of the besieged governments and promote further dissent. Eventually, as the government collapses and anarchy results, military forces under the guise of peacekeepers can then be employed to pacify the area, if desired, and a new government that is friendly to the United States and the West can be installed.[14]

The above excerpt describes how the Russian military envisions how the United States will conduct offensive military campaigns. Yet, it also reflects capabilities that the Russian military has used in Ukraine and will likely use in the future. In this strategy, the central feature of future warfare is the use of cyber capabilities to influence public opinion and public "knowledge." Cyber war now goes well beyond just hacking and degrading systems. As German military analyst Ralph Thiele argued, in modern war the opponent "will attempt to influence their target society's collective mindset so that their values and principles become challenged, their resolve weakened and consequently political objectives are abandoned or modified."[15] Once again if we go back to Sun Tzu's strategic advice, the goal of this indirect approach is to undermine "moral influence,"[16] meaning "that which causes the people to be in harmony with their leaders."[17]

Russian interference in the 2016 U.S. election follows the above pattern. The U.S. Central Intelligence Agency and the U.S Federal Bureau of Investigation are in agreement that Russia used a variety of cyber tools to sway the 2016 U.S. election in favor of Donald Trump [18] and, more generally, to undermine confidence in the U.S. electoral system.[19] Cyber espionage, hacking, internet trolls, false news reporting were used by Russia to undermine the credibility of Democratic Party's candidate Hillary Clinton and bolster the Republican Party candidate who advocated policies favored by, or at least more lenient toward, Russian leader Vladimir Putin and his foreign policy goals.

Russian security analyst Mark Galeotti described recent Russian "hybrid war" campaigns as the "blurring of the borders between state, paramilitary, mercenary, and dupe."[20] In this case, "dupe" is an important addition and points to the manufacture of "news" and "facts" by almost anyone with a computer. Widely available social media

permits almost anyone to report, film, or manufacture "facts" or "news" and make it available to the general public. The opponent then is set with the task of tracking and refuting false news reports that have been widely disseminated. Recent cases suggest that once a fake news report is widely reported it is difficult to refute it.[21] Russian use of cyber capabilities to inject ideas into U.S. public discourse and sway U.S. public opinion has been effective. Russian success in undermining public confidence in the electoral system and the integrity of democratic governance amongst a segment of the U.S. electorate is not only a short term strategic success for Russia, it is also an action that will have longer term negative consequences for U.S. domestic politics and U.S. foreign policy.

Cyber technologies are the core of modern society and the basis of personal and political power and influence. It follows that cyber is now a significant component in modern warfare. "Hybrid warfare," as Ralph Thiele argued, "is not limited to the physical battlefield. Any space available may be engaged. This includes traditional and modern media instruments."[22] The Russian analysis of the cyber component in warfare concluded the same:

> Beyond a shadow of a doubt, the aggressive side will be first to use nonmilitary actions and measures as it plans to attack its victim in a new-generation war. With powerful information technologies at its disposal, the aggressor will make an effort to involve all public institutions in the country it intends to attack, primarily the mass media and religious organizations, cultural institutions, nongovernmental organizations, public movements financed from abroad, and scholars engaged in research on foreign grants. All these institutions and individuals may be involved in a distributed attack and strike damaging point blows at the country's social system ...[23]

The head of Britain's MI6 emphasized the importance of addressing these new cyber strategies: "The risks at stake are profound and represent a fundamental threat to our sovereignty; they should be a concern to all those who share democratic values."[24]

Societal Resilience to Cyber Effects in Hybrid Warfare

Hybrid warfare presents two different kinds of threats to society: physical destruction and psychological effects. In the past, military strategy had focused on traditional concepts of warfare where specific targets were attacked in order to degrade or prevent their use by enemy forces. As illustrated above, now there is more attention to the psychological effects and the strategies used to alter public opinion and public support for political leaders. An analysis of statements of the Russian Ministry of Defense by Chekinov and Bogdanov pointed out that Russian strategic doctrine for New-Generation War focused on how opponents will use their cyber capabilities to

undermine or change societal beliefs and values. Russian military strategists envision that "new-generation war will be dominated by information and psychological warfare that will seek to achieve superiority in troops and weapons control and depress the opponent's armed forces personnel and population morally and psychologically. In the ongoing revolution in information technologies, information and psychological warfare will largely lay the groundwork for victory."[25]

The goal of an individual or group that is under threat is to maintain its existence whether this threat is physical or psychological. Societies that are resilient are more likely to survive in the face of danger and to recover if damaged. For states this means protecting a wide range of assets from infrastructure to the integrity of the relationship between citizens and leaders that lends legitimacy to political institutions. Societal resilience, as defined by Beatrice Pouligny of the U.S. Institute of Peace is: "the capacity of a group, community, or society at large to cope with stresses and disturbances as a result of social, political, and environmental change and to adjust while still retaining essentially the same functions and feedbacks by the people."[26] Societal resilience includes both the ability to handle or prevent physical damage as well as the ability to mitigate adverse psychological effects. Actions to build resilience against physical damage might include strengthening firewalls in computer networks; rebuilding any damaged infrastructure such as highways or power grids; providing good medical services so injured people will get well. Societal resilience must also include actions to handle or prevent adverse psychological effects through efforts to counter enemy propaganda and false news reporting; maintain trust between leaders, citizens and governing institutions; and ensure people are free from fear for their safety and survival. In essence citizens must feel that their government leaders are holding up their part of the social contract [27] and keeping them safe and secure.

The cyber component of hybrid warfare that includes the ability to alter people's beliefs, norms, and values can have significant consequences. Kaspars Galkins of the Latvian Ministry of Defense warned of this threat: "The worst case – by no means remote or improbable – is a hybrid threat actor that has full access to mass media and creates its own narrative to influence the hearts and minds of NATO populations."[28] ISIS/Daesh's skilled use of social media to recruit new members from countries around the world in order to turn these citizens into enemies of their own countries is an example of how powerful this "non-lethal" psychological component of hybrid warfare can be. On 24 August 2015, the United States used a drone strike to kill British citizen Junaid Hussein who was a top ISIS/Daesh hacker and computer expert.[29] The *Wall Street Journal* commented on the significance of this strike: "That he was targeted directly shows the extent to which digital warfare has upset the balance of power on the modern battlefield."[30]

In the aftermath of a hybrid attack the focus is most often on the loss of lives or physical destruction; for example, when we think about incidents such as the ISIS/Daesh terror attacks at the Charlie Hebdo offices on 7 January 2015, the Bataclan Theater in Paris on 13 November 2015, or the Brussels Airport attack on 22 March 2016. Physical damage also has psychological effects because it creates fear. In addition, adverse psychological effects are the product of propaganda campaigns, false news reporting, and other types of information warfare aimed at undermining a democratic society's trust in its leaders and in democratic beliefs and values. U.S. President Obama addressed this danger in his weekly address on 9 September 2016. In recalling the 9-11 attacks, he said: "As we reflect on these past 15 years, it's also important to remember what has not changed—the core values that define us as Americans. The resilience that sustains us. After all, terrorists will never be able to defeat the United States. Their only hope is to terrorize us into changing who we are or our way of life."[31] A resilient society must protect itself against adverse psychological effects including fear, distrust, and the breakdown of societal norms and values as well as from physical damage.

The Conundrum for Democracies

The cyber operations discussed earlier in this paper have the capacity to undermine fundamental ideas of democratic citizenship in a way that traditional military attacks do not. One of the key lessons learned from the strategic bombing campaigns in World War I, World War II, the Vietnam War, and other war theaters is that physical attacks against a population are more likely to result in a hardening of morale and increased patriotism rather than demoralization and surrender. Hybrid threats, particularly cyber threats, pose a conundrum for democratic governments trying to ensure that their societies are resilient. The ability of any democratic country to counter hybrid threats, in large part, depends on the willingness of its citizens to support government policies aimed at combating hybrid actors. In turn, some of the things that democratic governments would like to do to combat hybrid threats may undermine some of the basic freedoms that define what it means to be a democratic country. These basic freedoms include personal freedoms such as the right to privacy at home and the right to have private conversations and private correspondence that is not subject to government monitoring. On the one hand, government monitoring of personal conversations and personal activities is an action that is associated with the worst aspects of autocratic rule. On the other hand, if hybrid actors use cyber systems to cause damage then the only way to combat the threat seems to be through monitoring and using the same systems.

What is unique in the current era, and particularly in the case of hybrid threats, is that citizens of democratic countries have in some cases advocated, or been complicit in,

the undermining of their own democratic rights and freedoms. Government officials have argued that only by limiting some rights and freedoms can hybrid threats be effectively countered. Many citizens are willing to acquiesce. U.S. citizens' contradictory views on the U.S. National Security Agency's (NSA) widespread collection programs that were revealed by Edward Snowden illustrate the conundrum. It is widely known that the NSA collection programs monitored and stored (and continue to do so) the data from billions of phone calls each day as well as email messages, instant messages, Facebook posts, contact lists, videos, chat, file transfers, on-line social networking information, and other internet data.[32]

The U.S. government argues that NSA surveillance is necessary to protect U.S. citizens from terrorist attacks. However, U.S. citizens believe that the U.S. government has used the data it collected for purposes other than anti-terrorist operations. Despite this belief, they have acquiesced to the monitoring and surveillance of their own activities. A 2013 Pew Research Center poll found that only 30% of U.S. citizens think that U.S. courts provide adequate limits on what information the U.S. government is allowed to collect.[33] Meaning, that most citizens feel their rights are being violated. Since, the ostensible purpose for this extensive data collection is to prevent terrorist attacks, it might seem okay to give up some rights if you believe that the government is holding up its end of the bargain and using the data to protect you. However, this is not the belief of most people. The same poll found that 70 % of U.S. citizens believe that the U.S. government is using the data it collects for things other than anti-terrorism, namely they believe it is being used by the government for its own political purposes such as "to control/spy/be nosy" (19 %), "gather evidence on non-terror crimes" (16 %), "general purposes/monitoring" (14 %), "political agenda/targeting" (13%), and "whatever they want" (10 %).[34] What is surprising is that despite these beliefs in the illegality of data collection and the nefarious purposes that people believe it is being used for, only 44 % expressed a disapproval of the U.S. government's collection of phone calls, emails, and monitoring of internet activities.[35]

The Pew Research Center's poll results in 2014, the year after the Snowden revelations, also reflect the conundrum for U.S. citizens. In this poll, 74 % of Americans believed that they "should not have to give up privacy for safety"[36] but only about half (54 %) of them said that they disapproved of the NSA collection programs.[37] So, while the majority of people wanted their privacy safeguarded, many of those same people still approved of the NSA monitoring programs that violated their privacy.

U.S. citizens are not alone in acquiescing to increasingly intrusive government surveillance and monitoring. The governments of France, Germany, United Kingdom, Netherlands, Austria, Denmark, Finland, Norway,[38] and Switzerland[39] have all recently deliberated or passed laws allowing greater surveillance of their own populations. A recent analysis by journalist Hugh Eakin concluded, "the very qualities that

have made Sweden and Norway successful models of advanced democracy may also have made their populations more susceptible to government spying. In Norway, the government committee that put forward the mass surveillance legislation now before parliament has argued that such measures 'can be justified as necessary in a democratic society'."[40] This is an argument that seems to resonate and be accepted by citizens across Western democracies. This gradual relinquishing of democratic freedoms is a result of hybrid warfare strategies. It is a phenomenon that requires much more attention from scholars and democratic citizens alike.

Conclusion

Hybrid warfare presents a conundrum for Western democracies and their citizens. Increasingly, these governments have argued that their ability to counter cyber threats and "irregular" agents such as terrorists depends on the government's ability to monitor all forms of communication, information and social connections on the internet and through cellular networks. This paper has suggested that the willingness of citizens to support government surveillance programs will ultimately undermine the basic freedoms that define what it means to be a democratic country. Hybrid warfare has opened a new era for international politics and Western democracies as democratic governance is undermined not only by hybrid warfare threats, but also by actions taken by democratic governments to counter those threats.

Notes

[1] Based on the concept of "supercitizens" that was coined by David Rothkopf to describe private individuals with tremendous power and global reach. Supercitizens are the wealthiest people who have benefited from increasing wealth and income inequality of the 21st Century. These individuals have enough resources and influence to subvert state policy. See David Rothkopf, *Power, Inc.: The Epic Rivalry Between Big Business and Government – and the Reckoning That Lies Ahead* (New York: Farrar, Straus and Giroux, 2012), 5.

[2] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007), 9, footnote 2.

[3] John Mueller, *The Remnants of War* (Ithaca, NY: Cornell University Press, 2007).

[4] Hoffman, *Conflict in the 21st Century*, 8.

[5] Michael Aaronson, Yves de Kermabon, Sverre Diesen, and Mary Beth Long, "NATO Countering the Hybrid Threat," NATO/Allied Command Transformation, September 23, 2011, accessed December 17, 2016, http://www.act.nato.int/nato-countering-the-hybrid-threat.

[6] Damien Van Puyvelde, "Hybrid war – does it even exist?" *NATO Review*, May 7, 2015, accessed March 9, 2018, www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/.

[7] U.S. Department of Defense, *DOD Dictionary of Military and Associated Terms*, October 15, 2016, accessed December 17, 2016, www.dtic.mil/doctrine/new_pubs/dictionary.pdf.

[8] Charles K. Bartles, "Getting Gerasimov Right," *Military Review* 96, no. 1 (January-February 2016): 30-38, quote on p. 34, accessed September 17, 2016, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art009.pdf.

[9] Bartles, "Getting Gerasimov Right," 34.

[10] Sun Tzu, *The Art of War*, Samuel B. Griffith translation (Oxford: Oxford University Press, 1963), 77.

[11] Sergey G. Chekinov and Sergey A. Bogdanov, "The Nature and Content of a New-Generation War," *Military Thought: A Russian Journal of Military Theory and Strategy* 4 (2013): 12-23, quote on p. 16, accessed March 12, 2018, http://www.eastviewpress.com/Files/mt_from%20the%20current%20issue_No.4_2013.pdf.

[12] Valery Gerasimov (Chief of the General Staff of the Armed Forces of the Russian Federation), presentation at the Russian Ministry of Defense's Third Moscow Conference on International Security, 23 May 2014. Presentation slides and comments were recorded and made available by Anthony H. Cordesman, *Russia and the "Color Revolution" A Russian Military View of a World Destabilized by the US and the West (Key Briefs)* (Washington, D.C.: Center for Strategic and International Studies, 28 May 2014), accessed January 4, 2017, http://csis.org/publication/russia-and-color-revolution.

[13] Bartles, "Getting Gerasimov Right," 32-33.

[14] Bartles, "Getting Gerasimov Right," 32-33.

[15] Ralph D. Thiele, "Building Resilience Readiness against Hybrid Threats – A Cooperative European Union/NATO Perspective," *ISPSW Strategy Series: Focus on Defense and International Security* 449 (September 2016), 2.

[16] Moral influence is one of the five fundamental factors of war; the others are: weather, terrain, command, and doctrine. According to Sun Tzu's advice, "There is no general who has not heard of these five matters. Those who master them win; those who do not are defeated." *The Art of War*, p. 65.

[17] Sun Tzu, *The Art of War*, 63-64.

[18] Adam Entous and Greg Miller, "U.S. intercepts capture senior Russian officials celebrating Trump win," *The Washington Post*, January 5, 2017, accessed January 5, 2017, https://www.washingtonpost.com/world/national-security/us-intercepts-capture-senior-russian-officials-celebrating-trump-win/2017/01/05/d7099406-d355-11e6-9cb0-54ab630851e8_story.html.

[19] May Bulman, "FBI backs CIA view Russia intervened to help Donald Trump win presidential election," *Independent*, December 16, 2016, accessed December 17, 2016, http://www.independent.co.uk/news/world/americas/donald-trump-election-russia-cia-fbi-comey-clapper-a7480566.html.

[20] Mark Galeotti, "Russia's Hybrid War as a Byproduct of a Hybrid State, *War on the Rocks*, 6 December 2016, accessed December 18, 2016, http://warontherocks.com/2016/12/russias-hybrid-war-as-a-byproduct-of-a-hybrid-state/.

[21] For an example of how an ordinary person might spread fake news using social media, see: Sapna Maheshwari, "How Fake News Goes Viral: A Case Study, *New York Times*, 20 No-

vember 2016, accessed 5 January 5, 2017, http://www.nytimes.com/2016/11/20/business/media/how-fake-news-spreads.html. For an analysis of how mainstream news media propagate fake news see: Kalev Leetaru, "'Fake News' and How The Washington Post Rewrote Its Story on Russian Hacking of the Power Grid," *Forbes*, 1 January 2017, accessed January 6, 2017, http://www.forbes.com/sites/kalevleetaru/2017/01/01/fake-news-and-how-the-washington-post-rewrote-its-story-on-russian-hacking-of-the-power-grid/.

[22] Thiele, "Building Resilience Readiness against Hybrid Threats," 2.

[23] Chekinov and Bogdanov, "The Nature and Content of a New-Generation War," 17.

[24] Ben Farmer, "Head of MI6: Britain faces 'fundamental threat to sovereignty from Russian meddling'," *The Telegraph*, 8 December 2016, accessed December 17, 2016, http://www.telegraph.co.uk/news/2016/12/08/britain-faces-fundamental-threat-sovereignty-russian-meddling/.

[25] Chekinov and Bogdanov, "The Nature and Content of a New-Generation War," 16.

[26] Beatrice Pouligny, "The Resilience Approach to Peacebuilding: A New Conceptual Framework," United States Institute of Peace, accessed March 12, 2018, http://www.usip.org/insights-newsletter/the-resilience-approach-peacebuilding-new-conceptual-framework.

[27] In political philosophy, the social contract is the basis of governance whereby individuals agree to be governed and acquiesce to having laws enforced for the common good. Community leaders derive their legitimacy to enforce rules from the consent of community members. Community member give their consent to be governed in exchange for leaders providing them security and a stable, just, and organized society.

[28] Kaspars Galkins, *NATO and Hybrid Conflict: Unresolved Issues from the Past or Unresolvable Threats of the Present?* Master's Thesis (Monterey, CA: U.S. Naval Postgraduate School, 2012), 3.

[29] Brett McGurk (U.S. Deputy Assistant Secretary of State for Iraq and Iran), Twitter message, @brett_mcgurk, 9:40AM, 28 August 2015.

[30] Margaret Coker, Danny Yadron, and Damian Palette, "Hacker Killed by Drone Was Islamic State's 'Secret Weapon'," *Wall Street Journal*, 27 August 2015, accessed September 2012, 2016, http://www.wsj.com/articles/hacker-killed-by-drone-was-secret-weapon-1440718560.

[31] Barak Obama, "Upholding the Legacy of Those We Lost on September 11th," speech delivered on 9 September 2016, transcript accessed on September 25, 2016, https://www.whitehouse.gov/the-press-office/2016/09/10/weekly-address-upholding-legacy-those-we-lost-september-11th.

[32] Charles Arthur, "NSA scandal: what data is being monitored and how does it work?" *The Guardian*, 7 June 2013, accessed January 6, 2017, https://www.theguardian.com/world/2013/jun/07/nsa-prism-records-surveillance-questions.

[33] Michael Dimock, et al., *Few See Adequate Limits on NSA Surveillance Program but More Approve than Disapprove*, 26 July 2013, Pew Research Center, poll conducted on 17-21 July 2013, p. 1, accessed January 7, 2017, http://www.people-press.org/files/legacy-pdf/7-26-2013%20NSA%20release.pdf.

[34] Dimock et al., *Few See Adequate Limits on NSA Surveillance Program*, 4.

[35] Dimock et al., *Few See Adequate Limits on NSA Surveillance Program*, 1.

[36] Pew Research Center, *Beyond Red vs. Blue: The Political Typology*, 26 June 2014, p. 26.

[37] Pew Research Center, *Beyond Red vs. Blue*, p. 26.

[38] Hugh Eakin, "The Swedish Kings of Cyberwar," *New York Review of Books* 64, no. 1 (19 January 2017), 57.

[39] Hugh Eakin, "Switzerland votes in favour of greater surveillance," *The Guardian*, 25 September 2016, accessed September 25, 2016, https://www.theguardian.com/world/2016/sep/25/switzerland-votes-in-favour-of-greater-surveillance.

[40] Eakin, "The Swedish Kings of Cyberwar," 57.

About the author

Prof. Carol Atkinson retired as a lieutenant colonel from the U.S. Air Force in 2005. While in the military, she served in a wide variety of management and operational positions in the fields of intelligence, targeting, and combat assessment. During the Cold War she flew on the Strategic Air Command's nuclear airborne command post as a target analyst. During Operation Desert Storm (1991) she worked on the intelligence staff in Riyadh and, subsequently, on the contingency planning staff in Dhahran/Khobar, Saudi Arabia. While in the military, she taught at the Air Force Academy and the Air Force's Command and Staff College.

Atkinson holds a PhD in international relations from Duke University, an MA in geography from Indiana University, and a BS from the United States Air Force Academy (5th class with women). Carol was a postdoctoral research fellow at the Center for International Studies at the University of Southern California and a Senior Visiting Fulbright Scholar at Defense Advanced Research Institute, Sofia, Bulgaria in 2013. Atkinson's primary research focuses on U.S. military-to-military contacts as channels of international norm diffusion. She is also working on a project examining the influence of educational exchange programs on democratization and a project on the social construction of the biological warfare threat in the United States.