Hybrid Warfare:
Fighting Back With Whole-Of-Society Tactics

Note:

Hybrid Warfare is also known as grey zone conflict or unrestricted warfare. And these are just three of various terms now in circulation to describe the same phenomenon — multi-faceted attacks against a country that have serious implications for its national security and defence institutions. They may include military elements, but may also be mounted using cyber tools, public and commercial corruption, weaponization of legal systems, transnational organized crime, and disinformation campaigns, along with a host of other methods. Effective responses will demand an unprecedented level of cooperation between military, intelligence, cyber and other security experts in partnership with experts in the management of conflict in business, legal and public settings.

This issue of On Track examines the implications of the rise of hybrid warfare for Canada and other liberal democracies. It highlights the need to build resilience and to increase collaboration between the private sector, the public sphere, and other relevant entities (NGOs, universities, hospitals, municipalities and more). It assesses whether modern societies are adequately equipped to face these emerging threats, and stresses the need for enhanced cooperation and knowledge distribution.

This issue of On Track has been developed in collaboration with Project Seshat, a multinational group of experts organized to study and address the emerging threat of hybrid warfare. Find out more at https://www.project-seshat.org/.

All contributors to this issue are members of Project Seshat.

Contents

Chris Honeyman is managing partner of Convenor Conflict Management, a consulting firm based in Washington, DC. He has led or co-directed a 30-year series of R&D programs, advised many academic and practice organizations, and served as a professional neutral in more than 2,000 disputes. He is co-editor of seven books and author of over 100 published articles, book chapters and monographs.

Andrea Kupfer Schneider is Professor of Law and director of the Kukin Program for Conflict Resolution at Cardozo Law School in New York City. She has written numerous books, book chapters and articles on negotiation skills and styles, dispute system design, international conflict, and gender and negotiation. Her A.B. is from Princeton University and her J.D. is from Harvard Law School, and she was named the Outstanding Scholar by the American Bar Association Section of Dispute Resolution for 2017.

Calvin Chrustie, BA, BA (Honours), LLM is a senior security and critical risk consultant, specializing in the human element, negotiations (ransom), intelligence, investigations, national security and crisis response. Previously he served 33 years with the RCMP, specializing in transnational organized crime investigations, kidnap/extortion negotiations, crisis and conflict management. Calvin was also the Team Leader of Canada's International Negotiation Group, a group of specialized negotiators tasked with terrorist and hostage situations. He is now with the boutique advisory group, the *Critical Risk Team*.

Anne Leslie is Cloud Risk and Controls Leader—EMEA at IBM Cloud. She has spent much of her career at the intersection between financial services, regulatory policy and technology. At IBM her focus is on accompanying banks and financial institutions in securing their journey to public Cloud and adapting their cybersecurity operations to keep pace with a fast-changing threat landscape. She holds an Executive MBA from HEC Business School in Paris and the CCSP in Cloud Security from (ISC)^2.

Steven Desjardins retired as a Canadian Armed Forces Colonel and has since completed three years as a consultant to redesign Canada's Defence Intelligence enterprise. Previously, he served as the senior Intelligence officer in the Canadian Army and in the Canadian Joint Operations Command, and served a tour as senior Intelligence officer for human intelligence, counter intelligence and information security at SHAPE in NATO.

Sanda Kaufman is Professor Emeritus of Planning, Public Policy and Administration at Cleveland State University's Levin College of Urban Affairs. Her research spans negotiations and intervention in environmental and other public conflicts; social-environmental systems resilience; decision analysis; program evaluation; and negotiation pedagogy. She holds a B. Arch. and M.S. in Planning from Technion, and a Ph.D. in Public Policy Analysis from Carnegie Mellon University.

VOLUME 30 | FEBRUARY 2023

ON TRACK is the official journal of the CDA Institute. Through its pages, the CDA Institute promotes informed public debate on security and defence issues and the vital role played by the Canadian Armed forces in society. ON TRACK facilitates this educational mandate by featuring a range of articles that explore security, defence, and strategic issues that may have an impact on the Canadian strategic interests and on the safety of its citizens. The views expressed in ON TRACK are those of the authors and do not necessarily represent those of the CDA Institute.

CDA Institute / L'Institut de la CAD
900-75 Albert Street, K1P 5E7, Ottawa, ON
(613) 236 9903
www.cdainstitute.ca

Edited by:
Chris Honeyman & Andrea Kupfer Schneider

Hybrid Warfare: Fighting Back with Whole-of-Society Tactics

Chris Honeyman and Andrea Kupfer Schneider

Introduction

This special issue of *On Track* addresses some major questions now facing Canadian as well as other Western military forces: Why should hybrid warfare matter to the military?[1] How can the Canadian Armed Forces (CAF) enhance their capacity to respond to the evolving security risks posed by hybrid warfare? How can we increase collaboration between military and non-military actors to address this new form of conflict? Beyond awareness, what skills and tools do business leaders, lawyers, diplomats and politicians require? How can non-military initiatives enhance and broaden national defence resilience to this increasing threat? What barriers should stakeholders expect to encounter when dealing with this threat? How might these barriers best be addressed?

The October 6 CDAI webinar which led to the present issue reflected on the implications of this new type of warfare for Canada and other liberal democracies. It highlighted the need to build resilience and to increase collaboration between the private sector, the public sphere, and other relevant entities (NGOs, universities, hospitals, municipalities and more). In particular, panelists assessed how the CAF and other Western militaries are currently equipped to face these emerging threats, and stressed the need for enhanced cooperation and knowledge distribution between the armed forces and other entities with which they generally have had little contact.

Hybrid Warfare and Deliberate Confusion

One initial problem in creating teams to address this kind of conflict is confusion, even over the terms used to define it. Hybrid warfare is also known as grey zone conflict or unrestricted warfare. And these are just three

[1] Not all versions of hybrid warfare, at least in some definitions, include any element of the "kinetic" activity for which military forces, including the Canadian National Defence, were mainly designed. We will use "hybrid warfare" here to describe the full range of related activity, despite the fact that some professionals would define much of what we are talking about instead as "grey zone conflict." Some, particularly in the military, take the view that "the literature often depicts hybrid warfare and grey zone conflicts as two inter-related but distinct phenomena. In their view, hybrid warfare implies a conventional army augmented by a complex cyber/disinformation capacity, whereas gray zone refers to small tactical gains made 'under the threshold' over war." (Personal communication to authors from *On Track* editors, Jan. 2023.) However, it has been our experience that there is no consistency to be found in the use of these terms; even within military circles, other experts have used the term "hybrid warfare" where the above definition would have urged the term "grey zone conflict." See e.g. Tait 2019 (Tait is a former division chief for China and north-east Asia on the U.S. joint military staff.) See also the next section.

of various terms now in circulation to describe the same phenomenon — multi-faceted attacks against a country that have serious implications for its national security and defence institutions. They may include military elements, but may also be mounted using cyber tools, public and commercial corruption, weaponization of legal systems, transnational organized crime, and disinformation campaigns, along with a host of other methods. (Galeotti 2022; Tait 2019; Braw 2020; Qiao and Wang 1999. Further references will be found in the other articles in this issue.) For consistency, we will use "hybrid warfare" here (see also note 1)

In recent years an unfamiliar form of extreme international competition has become more evident. Some of its aspects are by now well known, such as interference in elections, or the rise of ransomware and other cyberattacks. (For more on this, see Anne Leslie's article in this issue.) In 2022 Russia's fresh invasion of Ukraine and the ensuing open warfare have become a focus of attention worldwide; but hybrid attacks by a variety of actors are still under way, and by some measures are even more numerous. In this issue, Sanda Kaufman distinguishes the new style of attack from long-used methods of undermining opponents in these terms:

> *....Perhaps a key difference between HW and historic deceptive methods of prevailing over enemies is the use of sophisticated technologies applied to ever more complex situations. HW technologies include acting covertly at great distances from the targets (e.g., the disabling of some of Iran's nuclear facilities using a computer virus), using information — correct or not — to target and rally various groups unaware of the real intent (e.g., youth destroying culturally valuable objects as a means of fighting against climate change), dividing and weakening various opponent groups (e.g., polarizing parts of societies), and even reaching out to the very young to addict them to social media activities and ideas that brainwash, or even to drugs.*

Less conspicuous than attacks on national-level targets and groups has been a whole array of more narrowly targeted gambits that take place in the private sector. Many of these appear to operate by perverting transactions that, to Western parties, may look like ordinary commercial dealings, such as in supply chains, licensing and other domains. There is increasing evidence that these attacks have become widespread, and that Western military, intelligence, police, and other security agencies are not (yet) well-structured to respond to such private sector actions in any strategic or coherent way. Furthermore, hybrid warfare campaigns change tactics frequently, and coordinate direct government actions with activity by private and nonprofit entities, as well as by using cyber tools, public and commercial corruption, lawsuits, transnational organized crime, religious entities, and disinformation campaigns, along with a host of other methods. Deception, and denial that any such attack is underway, are standard elements in creating an atmosphere of ambiguity, and in parallel, the attacker's desired state of mind among defenders: doubt and confusion. (For more on this, see Steven Desjardins 'article in this issue.)

When such an attack is even perceived, there are at least four common reactions to which different people may be drawn. Some incline toward threatening (or carrying out) acts of direct retaliation. Some may deny the existence of an attack, particularly when it is obscure, or seems too trivial to warrant a response, or when admitting its existence could expose embarrassing structural weaknesses or negatively impact commercial marketing strategies. Some see beefing up general defence expenditures as the answer. And others believe Canada and other Western countries should simply avoid dealings with any country suspected of mounting such attacks. It is also common to prefer one of these reactions for an attack by country A (perceived as an enemy) and a different one for country B (perceived as an ally.)

We believe that although each of the above four responses to hybrid warfare has its value in limited situations, none of them will work as a default rule. (For more on this, see Calvin Chrustie's article in this issue.) It is necessary to develop an overall approach, such that hybrid warfare attacks will be better understood as a class and *managed* on an overall level. There is a strong precedent for this view: our group, known as Project Seshat, is inspired by Cold War conflict management studies of how the West and the Soviet Union, over decades, could and did maintain something approximating a working relationship (including avoiding a nuclear war) even at the height of their bitterly fought conflict. The project therefore uses a conflict management perspective as its organizing principle.

We realize that to some military professionals this may at first seem counterintuitive, and we are certainly aware that in hybrid warfare the intentionally offensive conduct includes brinkmanship and weaponization of every available opportunity, including any possible negotiation process, though as we will describe we are applying "negotiation" in a specific way that does not necessarily include dealing directly with the opponent. And we should note right away that in one key respect the Cold War analogy can be misleading: the West-Soviet relationship was fraught and complicated, but compared to hybrid warfare as it exists now, the Cold War was somewhat structured.

"Negotiation" in Hybrid Warfare

Many who are unknowingly involved in hybrid warfare have little or no understanding of it, and even those who know of an attack are often badly informed as to what they can do. Our project seeks to help with that.

There is compelling evidence that the private and nonprofit sectors are major target areas in hybrid warfare — and often, they become the frontline responders and defenders. And so the critically important tactical and operational levels of responses tend to take place in highly dispersed corporate boardrooms, law offices, municipal government or university offices, etc.

However, they are even less well prepared for this than national governments. Our project's central focus is therefore on dealings of all kinds between Western firms (and NGOs etc.) and ostensibly private entities that may be controlled by hostile governments.

At the same time, the "negotiation" most directly relevant here is not what most people think of first, i.e. what happens directly at a bargaining table with "the parties." In hybrid warfare, direct negotiation between the attacker and the respondent is unlikely, with limited exceptions such as in ransomware attacks. But the kind of *preparation* that skilled negotiators make for any such encounter is, if anything, more relevant than ever, and needs to be addressed on a much broader level. In the hybrid warfare context, it will involve consultation and cooperation among different professional communities on who assumes what roles and responsibilities as part of a broader conflict management strategy. Several of the articles in this issue will have more to say about this.

In addition, it is becoming increasingly evident that the *"behind the table"* negotiations — in other words, the negotiations between many players who are nominally on your own side — are incredibly important in averting, preparing for, or responding to a hybrid warfare attack. A hybrid warfare attack on a company that has not prepared adequately can create an atmosphere of defensiveness and mutual recrimination up and down the senior corporate ranks, or the equivalent in other types of organization. And this disunity is exactly what the attacker wants. So *these* negotiations are what we are focused on.

Too often ignored or short-circuited, preparation here includes a careful analysis of parties with whom a company or nonprofit should even consider dealing. And because the real parties, goals and strategies in hybrid warfare are routinely disguised, that analysis is no simple matter. We believe that in future, military and other security agency professionals, who may have better access to early-warning sources that could help in this, can and should develop partnership roles with "domestic" firms, nonprofits, universities, hospitals, municipalities and other bodies which in the past have had little contact with the military. There are already some examples, such as, in the U.S., the FBI's Private Sector Office. But much more is needed, and our project exists, in large part, to help with this.

How Project Seshat Works

Project Seshat was organized starting in 2020 as a group of scholars and practitioners, for two main purposes: first, to *increase understanding* of a type of activity that is carefully designed to be as obscure as the attackers can make it; and then, to use that understanding to *help create methods* for averting attacks, and for mitigating harm when they occur.

Participants in the project are invited specialists in either negotiation / conflict management or security. The project is led by a steering committee of five, of which one member (Honeyman) serves as principal investigator. The initial working group of some fifty people come from the Five Eyes and a few other allied countries, and a larger array of subject fields.

In a globalized economy, business and NGO executives, and their representatives such as lawyers, are routinely engaged in negotiations of all kinds, with suppliers, customers, municipalities, potential merger partners and more. These dealings do not have to be visibly cross-border transactions to have hybrid warfare connotations. For example, if an apparently "domestic" firm a city government is contracting with — for water or other utilities, transport, its communication networks or a thousand other things — is in some hidden way influenced by an adversary government, the city might find itself on the wrong end of an attack without ever realizing the opponent's intention, or even its existence. In the widely-covered SolarWinds cyberattack, for example, the supply chain consequences affected thousands of companies as well as government agencies at all levels. Few of those entities had even realized they were at risk. That attack has been generally ascribed to the Russian foreign intelligence service. (Leslie 2023, in this issue.) And this example is of a cyber attack, a type which in some ways is *better* understood than attacks such as those which employ bribery or blackmail of a key company official, kidnapping-to-order performed by a transnational criminal network, or any of a host of deliberately obscure gambits. (See the articles by Steven Desjardins and Anne Leslie in this issue for other examples.)

Preparing professionals for this unfamiliar environment will not be simple. And as potential remedies begin to emerge, some will undoubtedly require governmental action. If the public at large can develop a better understanding of what is going on and what can be done about it, better public policy approaches are more likely. Here, even more than in other elements, civil-military collaboration seems essential to developing the necessary responses.

We have long believed in the importance of civil-military collaboration around concepts of conflict management, and our work in this area now has a nearly twenty-year history. We started working with a U.S. Army officer in the mid-2000's, and extended discussions with Leonard Lira, then teaching at the army's main military academy, West Point, started a chain of relationships that have made our current work possible. Lira's initial contribution to our *Canon of Negotiation Initiative,*[2] (Lira 2006) along with our initially separate discussions with Calvin Chrustie — then Canada's chief hostage negotiator, and now a contributor in this issue — led to convening the "wicked problems team" in the *Rethinking Negotiation Teaching*[3] project a few years later. That team in turn came to include, along with specialists in large-scale

[2] The Canon of Negotiation Initiative is described at https://www.convenor.com/canon-of-negotiation.html . We should also note that Lira's analysis deepened over the next decade. By the time he wrote for our *Negotiator's Desk Reference* he had served two tours in Iraq and one in Afghanistan (by then, as director of operations for all NATO forces in Kabul.) As one result, his treatment of the military's use of negotiations was greatly extended in Lira 2017. For how this military expertise integrates with many other fields, see Honeyman and Schneider 2017, and Schneider and Honeyman 2006.

[3] Described at https://www.convenor.com/rethinking-negotiation-teaching.html .

conflict — its military and police officers, and a professor of peacebuilding at a Mennonite university — a wider array of experience that turned out to be relevant, including an ombudsman whose daily fare was disputes between 20,000 scientists (each of whom, he said, had "a direct line to Truth"), a London-based theater director, and still more, such as a South American politician whose experience included serving as a big-city mayor, and later, as president of his country.

Together, their output laid the basis for understanding how "wicked problems" operate in conflict and its management, and what an intervenor — military or otherwise — might usefully do about it. Our current project would not have been possible without that previous work. However, wicked problems are inherently subtle, and take time even to describe; a discussion of how they operate in conflict settings is beyond the scope of this brief introduction, so we will refer interested readers to a note below, [4] and to the references therein.

What Can We Do?

With the background described above, we think Project Seshat is well placed to help set up parallel groups within some of society's main constituencies (including the military, business groups, bar and academic associations and more), specifically chartered to make collaboration across "silos" easier. We can help create structures that will foster continuing interchange among them. We can help to validate that effort in the eyes of key groups such as political bodies. And we can develop feedback loops so that everyone involved, including us, has the best opportunity to learn from others 'experiences (including difficulties) across such a network.

Articles in this Issue

The articles in this issue focus in detail on a range of hybrid warfare issues which are alluded to here only briefly. Thus Calvin Chrustie identifies the gaps *between* our society's different elements — at least some of which are quite robust in and of themselves — as particularly fruitful targets for hybrid warfare attackers. Anne Leslie focuses on the need to build trust between military and other security forces, and corporations and other civil targets, as well as for corporations to take a broader view than is now typical, if cyber attacks are to be addressed better than they are at present. Steven Desjardins reviews the recent history of hybrid attacks, and finds that of all the major threat actors, it is China that is

[4] Honeyman and Coben (2010) boil down a composite set of characteristics of wicked problems, derived from Rittel and Webber (1973), Ritchey (2005-2008) and Conklin (2005). Our projects 'series on wicked problems in conflict settings, and the related problem of how to get teams of very diverse people working effectively together on such slippery issues, goes into much more detail in Chrustie et al. (2010), Docherty (2010), Lira (2010), Docherty and Chrustie (2013), Docherty and Lira (2013), Gadlin, Matz, and Chrustie (2013), Honeyman and Parish (2013), and Lira and Parish (2013). These practice-experience-centric writings are all available in PDF form without charge via the *Rethinking Negotiation Teaching* project pages at www.convenor.com, and map well onto a more academic treatment of intractable conflict by scholars we have also been privileged to work with, in Coleman et al. (2006), Lewicki, Kaufman, and Coben (2013), Coleman, Redding, and Fisher (2017a, 2017b), and Coleman and Ricigliano (2017).

most worrisome and that deserves the most sustained attention. And Sanda Kaufman brings to bear deep experience with other types of "wicked problems" and shows the extent to which our society has already developed a surprising range of useful tools, ready to adapt to the new purpose: so we may be a bit further along toward effective responses to hybrid warfare than we think.

To conclude, among many groups across our society with whom we hope to develop ongoing partnerships to address hybrid warfare, the military is high on our list. If you are interested in exploring this subject further, we and our Project Seshat colleagues would like to hear from you. We can be reached at honeyman@convenor.com and andrea.schneider@yu.edu.

References

Braw, Elisabeth. 2020. "Greyzone and Non-Kinetic Threats: A Primer." Available at https://www.aei.org/wp-content/uploads/2020/10/Elisabeth-Braw-Greyzone-Non-Kinetic-Threats-Primer.pdf?x91208 (see also https://www.aei.org/profile/elisabeth-braw/ for an up-to-date selection of Braw's frequent articles.)

Chrustie, Calvin, Jayne Seminare Docherty, Leonard Lira, Jamil Mahuad, Howard Gadlin, and Chris Honeyman. 2010. Negotiating Wicked Problems: Five Stories. In *Venturing Beyond the Classroom*, edited by Chris Honeyman, James Coben, and Giuseppe De Palo, 449–480. St. Paul, MN: DRI Press.

Coleman, Peter, Lan Bui-Wrzosinska, Robin R. Vallacher, and Andrzej Nowak. 2006. Protracted Conflicts as Dynamical Systems. In *The Negotiator's Fieldbook*, edited by Andrea Kupfer Schneider and Chris Honeyman, 61–73. Chicago: American Bar Association.

Coleman, Peter, Nicholas Redding, and Joshua Fisher. 2017a. Understanding Intractable Conflicts. In *The Negotiator's Desk Reference (vol. 2)*, edited by Chris Honeyman and Andrea Kupfer Schneider, 489–508. St. Paul, MN: DRI Press.

---. 2017b. Influencing Intractable Conflicts. In *The Negotiator's Desk Reference (vol. 2)*, edited by Chris Honeyman and Andrea Kupfer Schneider, 509-527. St. Paul, MN: DRI Press.

Coleman, Peter, and Rob Ricigliano. 2017. Getting in Sync: What to Do When Problem-solving Fails to Fix the Problem. In *The Negotiator's Desk Reference (vol. 2)*, edited by Chris Honeyman and Andrea Kupfer Schneider, 467-488. St. Paul, MN: DRI Press.

Conklin, Jeff. 2005. Wicked Problems and Social Complexity. In *Dialogue mapping: Building Shared Understanding of Wicked Problems*, edited by Jeff Conklin. New York: Wiley.

Docherty, Jayne Seminare. 2010. "Adaptive" Negotiation: Practice and Teaching. In *Venturing Beyond the Classroom*, edited by Chris Honeyman, James Coben, and Giuseppe De Palo, 481-504. St. Paul, MN: DRI Press.

Docherty, Jayne Seminare, and Leonard L. Lira. 2013. Adapting to the Adaptive: How Can We Teach Negotiation for Wicked Problems? In *Educating Negotiators for a Connected World*, edited by Chris Honeyman, James Coben, and Andrew Wei-Min Lee, 383-418. St. Paul, MN: DRI Press

Docherty, Jayne Seminare and Calvin Chrustie. 2013. Teaching Three-dimensional Negotiation to Graduate Students. In *Educating Negotiators for a Connected World*, edited by Chris Honeyman, James Coben, and Andrew Wei-Min Lee, 443–474. St. Paul, MN: DRI Press.

Gadlin, Howard, David Matz, and Calvin Chrustie. 2013. Playing the Percentages in Wicked Problems: On the Relationship Between Broccoli, Peacekeeping, and Peter Coleman's *The Five Percent*. In *Educating Negotiators for a Connected World*, edited by Chris Honeyman, James Coben, and Andrew Wei-Min Lee, 475–510. St. Paul, MN: DRI Press.

Galeotti, Mark. 2022. *The Weaponization of Everything: A Field Guide to the New Way of War*. New Haven: Yale.

Honeyman, Chris and James Coben. 2010. Navigating Wickedness: A New Frontier in Teaching Negotiation. In *Venturing Beyond the Classroom*, edited by Chris Honeyman, James Coben, and Giuseppe De Palo, 439-447. St. Paul, MN: DRI Press.

Honeyman, Chris and Rachel Parish. 2013. Choreography of Negotiation: Movement in Three Acts. In *Choreography of Resolution: Conflict, Movement and Neuroscience*, edited by Michelle LeBaron, Carrie MacLeod, and Andrew F. Acland, 73–85. Washington, DC: ABA Books.

Honeyman, Chris and Andrea Kupfer Schneider. 2017. *The Negotiator's Desk Reference*. Two volumes. St. Paul, MN: DRI Press. (Web edition: NDR Books, www.ndrweb.com)

Lewicki, Roy, Sanda Kaufman and James Coben. 2013. Teaching Wickedness to Students: Planning and Public Policy, Business, and Law. In *Educating Negotiators for a Connected World*, edited by Chris Honeyman, James Coben, and Andrew Wei-Min Lee, 511-537. St. Paul, MN: DRI Press.

Lira, Leonard. 2006. The Military Learns to Negotiate. In *The Negotiator's Fieldbook*, edited by Andrea Kupfer Schneider and Chris Honeyman, 675-685. Chicago: American Bar Association.

Lira, Leonard. 2010. Design: The U.S. Army's Approach to Negotiating Wicked Problems. In *Venturing Beyond the Classroom*, edited by Chris Honeyman, James Coben, and Giuseppe De Palo, 511-528. St. Paul, MN: DRI Press.

Lira, Leonard. 2017. Negotiation in the Military. In *The Negotiator's Desk Reference (vol. 2)*, edited by Chris Honeyman and Andrea Kupfer Schneider, 327-353. St. Paul, MN: DRI Press.

Lira, Leonard and Rachel Parish. 2013. Making It Up as You Go: Educating Military and Theater Practitioners in "Design." In *Educating Negotiators for a Connected World*, edited by Chris Honeyman, James Coben, and Andrew Wei-Min Lee, 419-441. St. Paul, MN: DRI Press.

Qiao, Liang and Xiangshui Wang. 1999. *Unrestricted Warfare*. Beijing: People's Liberation Army Publishing House. (For recommendations of English translations of Qiao and Wang, see "Précis: Unrestricted Warfare," Military Review, Sept.–Oct. 2019, available at https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2019/Precis-Unrestricted-Warfare/)

Ritchey, Tom. 2005-2008. *Wicked Problems: Structuring Social Messes with Morphological Analysis*. Swedish Morphological Society. Available at www.swedmorph.org (last accessed June 28, 2010).

Rittel, Horst. and Melvin M. Webber. 1973. Dilemmas in a General Theory of Planning. *Policy Sciences* 4: 155–169.

Schneider, Andrea Kupfer and Chris Honeyman. 2006. *The Negotiator's Fieldbook*. Chicago: American Bar Association.

Tait, S. 2019. Hybrid warfare: The new face of global competition. Financial Times, October 14. Available from https://amp.ft.com/content/ffe7771e-e5bb-11e9-9743-db5a370481bc.