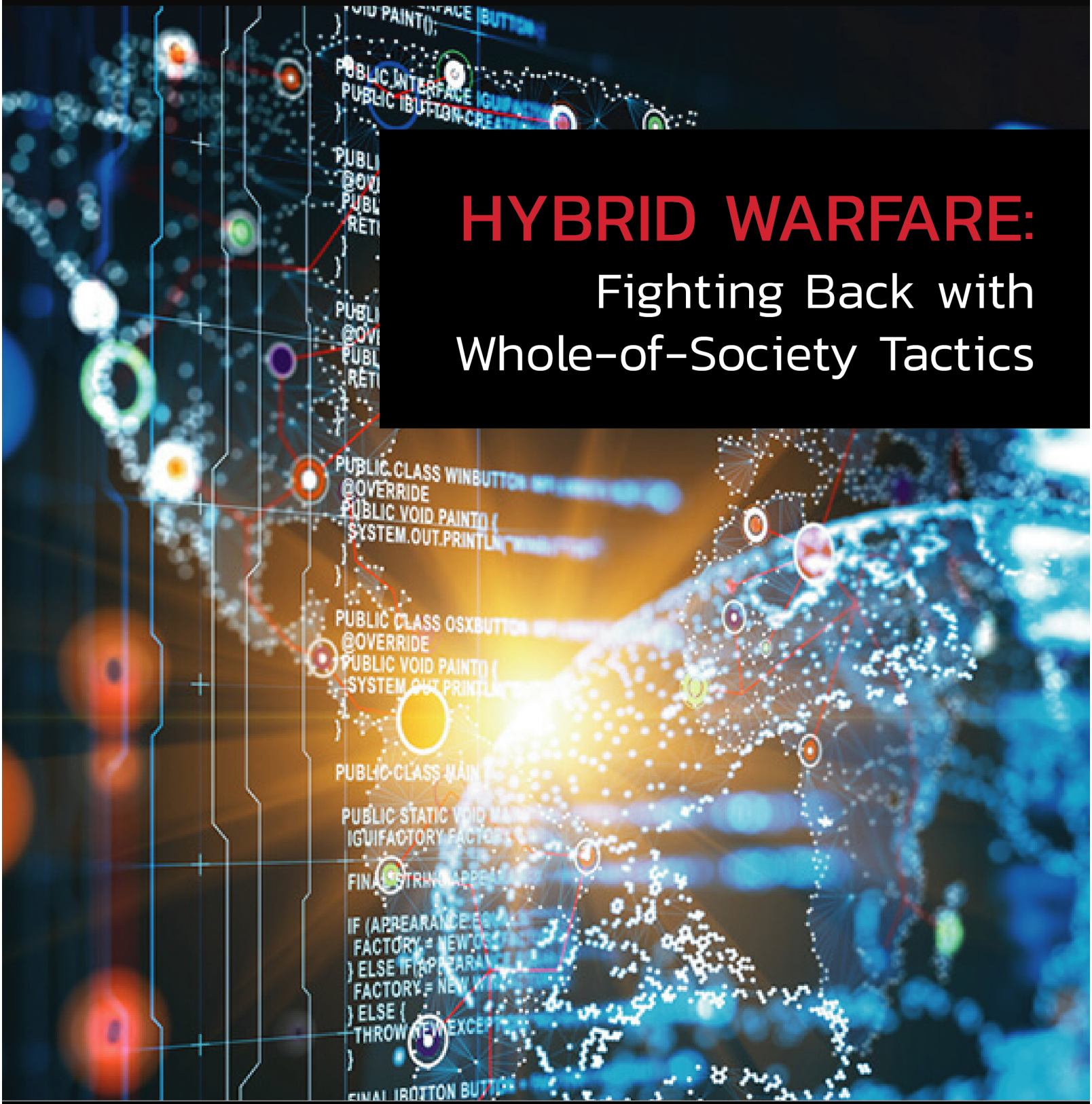
ON TRACK

CONFERENCE OF DEFENCE ASSOCIATIONS INSTITUTE | L'INSTITUT DE LA CONFÉRENCE DES ASSOCIATIONS DE LA DÉFENSE



HYBRID WARFARE:

Fighting Back with Whole-of-Society Tactics

VOLUME 30 | FEBRUARY 2023

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

Overview

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/.

Contributors

All contributors to this issue are members of Project Seshat:

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.

Table of Contents

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

[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.

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. (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

[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 .

include, along with specialists in large-scale 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

[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).

of all the major threat actors, it is China that is 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.

Mind the Hybrid Warfare Gap

Calvin Chrustie

Introduction

Take a ride on the London Underground, and at every station you will hear the same warning, over and over: "Mind the Gap." With more than a century's experience, the Underground management knows well the variety of sources of possible accidents, including being hit by a moving train or a simple slip-and-fall on the platform. But the warning reflects accumulated knowledge: the major risks have to do with the *spatial gaps between large structures*, in this instance the space between a train and the platform (Brown, 2022).

This article will focus on the concept of the *'gaps'* in our analysis and responses to hybrid warfare, including where there may be vulnerabilities—but also opportunities. These include not the possibility of better defences, but perhaps even offensive opportunities in business, law, diplomacy and in politics. This could include both reactive and strategic initiatives using negotiation and broader conflict management considerations.

In examining the current situation of hybrid warfare, our project is designed to bridge the gaps between awareness and expertise; between civilian and military response; between reaction and proactive

negotiation planning; between kinetic responses and strategic conflict management approaches; and so forth.

Now, perhaps consider the X Factor, "a variable in a given situation that could have the most significant impact on an outcome", as described by the Oxford English Dictionary. I will argue that these concepts can be useful in assessing hybrid warfare and its relationship to conflict management, including negotiations. Perhaps developing, adopting, and implementing conflict management strategies and enhanced negotiation responses may not only aid democratic countries, but may also be an "X Factor" and a key to effective responses to hybrid warfare—if we can end their gross neglect in both theory and practice.

Both the "Mind the Gap" subway warnings and Project Seshat focus on the acute threat created by the spatial area between large structures. In the "Mind the Gap" threat, this spatial area is the distance between two large structures, i.e. '*the platform and the train*'. The public and others tend to focus on the large structures. However, it is the more subtle space between where the most acute threat lies. As noted above, the familiarity of the 'Mind the Gap 'phrase is telling as to the societal knowledge of the threat in the Underground context. Perhaps we can build on this, as in the UK, in Canada and other Western democracies alike, historically little attention seems to have been given to this spatial gap in hybrid warfare.

In attempts to respond to hybrid warfare, as with the subway scenario, the large structures are often what attracts the attention of most, causing the 'gap 'to be the more acute threat. The analogy here is to the large structures of the "adversary" i.e. China, Russia, Iran and North Korea. In parallel, there is a focus on the large structures in our own society, i.e. our own military, defense, intelligence, and law enforcement agencies—on the surface, a logical enough focus, as these entities are explicitly designed to protect our citizens, institutions, and democracy.

Thus, a quick review of the media's more relevant headlines on any given day in 2022 is likely to show that most of us have focused on the issues and threats and capabilities of either our adversaries (Russia, China etc.) or a critical analysis of our own institutions (i.e. the military – better weapons, intelligence – more powers, and law enforcement – more resources).

The Gaps

The subtle but acute gaps in between get much less attention. Recently, however, FBI Director Christopher Wray recognized this gap and spoke to it explicitly, in discussions with senior MI5 and FBI officials in the summer of 2022, as the Director of the FBI addressed key British business leaders in London. He stated:

> "the Chinese government poses an even more serious threat to Western business than even many sophisticated businesspeople realize…..the Chinese Government sees cyber as the pathway to cheat and steal." […] "In addition to traditional and cyber enabled thievery, there are even more insidious tactics they use to essentially walk through

> your front door - and they will rob you…..by making investments and creating partnerships that position their proxies …. they use elaborate shell games to disguise these efforts from foreign companies …including shutting off data that used to enable effective due diligence….a 2017 law allowed them to force Chinese employees in China to assist in Chinese intelligence operations" (Wray 2022).

This is not merely a gap where "attack surfaces" exist for hybrid warfare, but more concerning, where there is a lack of awareness and defensive capabilities, effective conflict management strategies, negotiation skills or supportive tools, as outlined by several other writers in this issue. By the same token, more encouragingly, there are now some key opportunities to enhance awareness and leadership capabilities in conflict management, negotiation, and other non-kinetic means in this space.

Ret'd Canadian Army Colonel Steven Desjardins in his article in this issue has highlighted one element worth repeating: "What has changed is the exponential growth in societal interfaces that constitute key vulnerabilities exploited by hostile nations to wage hybrid warfare, as well as the ambiguity, speed, breadth, persistence and reach now afforded to hostile actors" (Desjardins, in this issue). But where are these societal interfaces, and who needs to engage? The military, intelligence agencies, police? Let's look at one of the more detailed classifications of threat activities, as prepared by Casey Fleming of the security firm Black Ops:

In this analysis, as with many classification and terminology frameworks relative to hybrid warfare, there can always be varied interpretations and differing analysis. However, if Fleming's typology is accepted as "good enough for immediate purposes," it reveals an interesting analysis. First, *only ten (10) of forty-two (42) threat activities fall solely within the military's traditional sphere of influence*. That equates to less than twenty-five percent (25%). More interesting still is, *who* then is left responding to or managing these threat activities, these conflicts? As the Director of the FBI, Mr. Wray suggests, the private sector, with C-Suites and their legal advisors most often, as noted in this article.

Hybrid Warfare – Is there a Role for Conflict Management and Negotiation?

The idea that 'war 'can be addressed at least in part through conflict management and negotiations has been carefully outlined by Leonard Lira (U.S. Army Colonel, ret.) in

"Negotiation in the Military" (Lira 2017). Lira wrote following years of experience in U.S. military operations in Afghanistan, Iraq, Syria, and North Africa, culminating in a period as director of operations for all NATO forces in Kabul. He noted: "If there is one thing that the U.S. military has learned in the last decade-plus of conflict, it is that force alone is insufficient to win peace." Even in the early 1990's, Lira stated: " ….the military found itself interacting with a multitude of organizations and individuals in operations that necessitated a safe resolution to volatile situations".

With the evolution of hybrid warfare and the expansion of conflict away from the traditional battlefield, we find ourselves dealing with threats, disputes, and threat actors, including their proxies, which have spilled over into corporate boardrooms, law offices, city halls, diplomatic discussions and in the political arena. In these environments, the common interactions are not with traditional weapons but with dialogue, negotiations, and mediation, often within a general "conflict management" framework. Conceptionally, could these negotiations operate in a defensive and perhaps, even in an offensive mode? While there appears to be little past consideration of this possibility in business, law, diplomatic and political science schools, I believe there is opportunity here.

Over more than a generation now, common teachings and practice in conflict management and negotiation, particularly in the Western democracies, have stressed looking for a "win-win'" collaborative outcome. However, we know our society's adversaries have a more distributive mindset. It is all too easy for those with a 'win-win ' orientation to lose out when facing a ruthless opponent who has no interest in interest-based principles of negotiation. (Cristal 2017, and citations therein.)

Yet Lira has laid out how even amid a traditional "kinetic" campaign, the application of "conflict management effective strategies and negotiation" can be highly effective. I suggest this is also true in the contemporary setting, of responding to the global hybrid warfare campaigns maintained by powers such as China, Russia, Iran, and North Korea. Like my Project Seshat colleague Lira, I also come from a background that includes peacemaking operations, volatile conflict, and extensive negotiation engagement with nefarious entities in society, including warlords, hostile political leaders, terrorist organizations and transnational organized crime entities. Congruent with Lira's experience in a variety of conflict situations, three decades of my own practice would suggest that many of these situations have lacked any effective conflict management or the corresponding strategic negotiation considerations.

Based on years of working in "domestic" settings where international warfare was playing out, including with "C suites", law firms, diplomats, and political leaders, I believe that in many instances, more effective strategic approaches to conflict management and negotiations could have been applied, notwithstanding the complexities of involving all key stakeholders.

Conflict management considerations and negotiation strategies provide significant

opportunities to prevent, mitigate, and resolve these threats to Canadian society and the global community. This understanding has been hard-won: when I first served in peacekeeping operations in the Bosnian war in the 1990s, these ideas first appeared as an afterthought or as secondary considerations. Only with time did I recognize that they were central to formulating an effective suite of responses. (Chrustie et al 2010; Docherty and Chrustie 2013; Gadlin, Matz and Chrustie 2013)

In short, whether one is looking at cyber attacks, mergers and acquisitions, insider threats or other elements in the above table, normal business processes, such as negotiations, are significantly impacted by many of these threats. For example, if private sector cyber activities are monitored by illicit cyber activity, or insider threats compromise management's internal deliberations, negotiation processes will be devoid of the expected confidentiality. Or if even identifying who the other party *is* will sometimes be hard (as they may be disguised by proxies), this undermines much of traditional negotiation planning and strategy.

Thus, these two factors alone can make it difficult to identify the other party's real *'interests',* to assess and solidify sustainable agreements, and lastly, to build trust. When one side is, directly or indirectly, routinely engaged in destructive and unethical activities, integrity of any ongoing negotiation is compromised. Traditional training and strategies in the field of negotiation may not be broad or deep enough to effectively deal with these asymmetrical negotiation and dispute issues.

So far, I have merely addressed *business* challenges. Yet similar challenges and implications cascade into the legal, diplomatic, and political arenas, to name only a few more.

And if these business and other civil leaders aren't military, and don't have weapons, what responses *are* there to navigate, mitigate and excel in this highly polarized and threat filled theatre of operation? The first and most obvious option is to avoid dealing with such parties. But like many other aspects of hybrid warfare, avoidance is not always possible. And as we know from traditional lessons in conflict management, even when avoidance is possible, it may not be the most effective response. Parties often have a competing interest in continuing engagement, for financial or other reasons, even though the relationship is fraught with risks.

And the alternatives are, then, what? Perhaps: to engage, but to do so *utilizing a better toolkit—with a range of dialogue options, strategic conflict management considerations and non-conventional negotiation processes, intertwined with risk and security considerations*.

Are most practitioners even equipped for this, educated, trained? One could argue, if over seventy-five percent of the threats (75%) fall on corporate offices, law firms, political offices (including municipal, provincial, indigenous, and federal) and diplomats engaged with the threat actors, as per Fleming's typology (https://blackopspartners.com/resources/), this

should be a priority in continuing as well as general professional education, in a wide variety of fields. In this issue, Honeyman outlines a set of ways Project Seshat may be able to help.

The Canadian Battlefield of Hybrid Warfare

Even looking at Fleming's "Military" activities, many of these touch on the civilian entities of our nations, including law firms, business leaders and others. While the military is empowered to "defend" outside Canada in accordance with the Canadian military legal framework, it has limited powers to operate internally (Canadian ***National Defense Act, 1985***). What does this mean for Hybrid Warfare? The Canadian Security Establishment (CSE), the Canadian Security and Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP), FINTRAC, the Canadian Border Services Agency (CBSA) and host of others have roles, which often overlap and in which bureaucratic rivalries are always possible. Yet what strikes me most from three decades of working within policing in Canada and abroad, and with other government agencies, is that our domestic institutions 'capability in mitigating these threats is limited'.

This is due to a complex web of issues. This includes a legal system designed to protect individual rights, and relatively weak on contemporary and practical provisions to ensure the protection of democratic institutions, along with the sovereignty and integrity of our nation. So, are the military, the intelligence or law enforcement communities really the ones who are most likely to encounter these threats?

While most of the current discussion, funding and strategies are focused on the government and its various branches, in my recent private sector experience I have observed a general lack of focus, engagement, and strategy to support the private sector. In short, if the battlefields for hybrid warfare are corporate boardrooms and law offices, should there be a shift in both strategy and operations in defense and offense?

This is the genesis of Project Seshat. After thirty years 'work within the government security and intelligence apparatus, it was not until I moved into the private sector as a risk, security, and intelligence consultant that I realized (congruent with the Fleming typology) that most national security issues were being dealt with by *'first responders.'* These first responders were not police or other security people, they were lawyers, corporate leaders, politicians, and diplomats. Most of these are struggling to defend themselves and their interests. None have any kinetic capabilities; they have limited access to national intelligence reports, and most concerning, they have minimal opportunity to engage the public sector meaningfully. Equally concerning is a trust factor, including a perception and level of awareness that our public institutions have minimal capabilities, are impeded by legal constraints as well as bureaucracy, and are rife with conflicts of interest and a system that appears to create the perception of "us vs them" between the private and public sector.

Things seem somewhat better in these respects south of the Canadian border. At least recently, U.S. agencies have more actively engaged with the private sector, with the FBI running defensive operations with the private sector, the military supporting transnational anti-crime operations (both with US domestic agencies and even Canadian ones), and where threats are more clearly and regularly shared with the public—even to the extent of working closely with Canadian domestic agencies in operations. In Canada, meanwhile, law firms, corporate leaders and others have had to rely on risk and security officials, including entities from our allies, to support and protect them. In some cases, these risk and security consultants have *had* to rely on foreign law enforcement and intelligence agencies to protect Canadian businesses, law firms and their clients.

Three brief case studies demonstrate how important conflict management and negotiations are in hybrid warfare. These three cases are all recent, and are all infused with a multitude of conflicts, with conflict and negotiation channels forming a complex web of dialogue. These demonstrate that like other forms of war, having a strategy to manage the conflict is essential. (Some of the details of these cases have been changed to protect the identity of the victims.)

1) Lawfare: Canadian Journalist vs China – a well-known journalist in Canada, known both nationally and internationally for reporting on threats and activities of China against Canada, is confronted by several lawsuits with the object of suppressing his reporting on hybrid warfare. Obviously, there is conflict between the reporter and China. Also, between the media firm and China. A series of ongoing litigations (i.e., disputes) have been launched against the journalist for alleged defamation of Canadian corporations. An assessment by the victim suggests the litigation is being funded by associates of the Communist Party of China. This kind of threat activity is known as" lawfare," a/k/a weaponizing the law and using it against civilians. When employed by foreign states, it is obviously an extension of the larger conflict. But it essentially pits the entire Chinese state against a Canadian journalist and his / her company—and no military or security officials are consulted or looped into this "private" process. The litigation process, obviously fuelled by virtually unlimited funds from China (directly or indirectly) makes litigation a virtually cost prohibitive process. So, is the alternative resolving the case (like many litigations) through informal dispute resolution processes and negotiations? While I have simplified the case and the dynamics, does it come down to a complex series of negotiations between the journalist, the various legal teams and corporate entities, and China's proxies? Perhaps not: against this are a variety of considerations including a huge power imbalance in the negotiations, and associated intimidation; a threat-infused context; the lack of confidentiality (dirty tricks including likely electronic

surveillance of all the Western participants by Chinese intelligence agents), and the impossibility to even engage directly with the primary parties, who are merely using proxies in the negotiation. Thus, the case shows the role and challenges in negotiation within the legal and business sector. Yet are there perhaps some opportunities here, along with the daunting negotiation challenges?

2) Hostage Taking: Illegal Detention of Canadians 2018–2022. Due to the recency and publicity of the "two Michaels'" illegal detainment, a/k/a the kidnapping of Michael Kovrig and Michael Spavor as hostages, this case is relatively well known. It highlighted the complexities conflict negotiation posed to the legal and NGO world, as well as business, diplomatic and political entities, when negotiating with China and their proxies. Again, an immense power imbalance of Canada vs China was observed. Canadians referring to the dispute tended to treat it as a diplomatic issue, vs. what it really was: i.e. part of the overall context of hybrid warfare. The case included strategic and dirty tactics, such as trade boycotts on the vulnerable and ill-informed farming and political community, with the "pork trade" frozen. Those impacted (and their business and political leaders) naively started out thinking this was a "trade war," and thus failed to grapple with the real issues entirely. Meanwhile lawyers, business leaders and others, not appreciating the power of China's SIGINT and cyber capabilities to monitor the negotiation processes and dispute resolution strategies, inadvertently provided China with a robust picture of Canada's negotiating weaknesses. Added to this were the Chinese likely leveraging the cyber domain, advancing misinformation and disinformation through cyber bots, 'useful idiots' and insider threats within Canadian political institutions and academia. (It is fair to note that the complexity of this only increases with another party to the dispute, the United States, also likely monitoring the negotiation processes and influencing them through a variety of means.) Lastly, most Canadian participants, to my eye, appeared to fall short of recognizing that these were 'conflict negotiations' in the context of a global ongoing hybrid war. Yet other ongoing attacks by China during these negotiations in Canada were semi-public: they included the alleged weaponization of fentanyl; ongoing espionage cases; military intimidation by the Chinese Airforce against the Canadian Navy; daily cyber-attacks on Canada, etc. All of these impacted the negotiations and were critical aspects of the negotiation 'context' that influenced the ongoing negotiation processes.

3) Cyber Attack – During the course of the current Russia/Ukraine war, Russian government-affiliated cyber threat

actors have targeted Canadian businesses suspected of supporting Ukraine. Extortion for ransom, and subsequent negotiations between business leaders, various law firms, U.S. and Canadian government entities and cyber companies were ongoing. Thus, the conflict between Ukraine and Russia spilled into the corporate and law offices of Canadian cities, and the resolution was expected through negotiations and ransom payments. Again, the power imbalance dynamics were stark: a Russian state-affiliated cyber gang against Canadian business leaders and their legal representatives, who were confined by law and rules in their negotiation process, while the Russian networks used extortion and intimidation, disregarded any privacy laws, and likely had insider insight into various entities among the Canadian parties in negotiations. This was just one of thousands of likely cyber incidents requiring negotiations with the threat actors, including with all stakeholders and even with other nations, e.g. the United States' FBI. Within these various negotiations with the threat actors, amongst the stakeholders working through policy and legal disputes, was there a pre-existing strategy on cyber ransom, foreign state attacks, business, and legal responses to these disputes? The simple answer is: there was none.

What do "Mind the Gap', Lira's writing, Fleming's typology, and the three cited cases tell us about hybrid warfare? In essence, together they give us an understanding that most of the threat activity is occurring in a space where (deliberately) the most acute impact and risks to Canada and the West in general lie within *the spatial gaps between* our societies 'various sectors, civilian and military, legal and civil, municipal / provincial, and corporate and more. Who in Canada is managing Hybrid Warfare activities in Canada? Are there logistics, strategy and command and control? Are the front-line responders aware of the activities, in their daily interaction with Chinese, Russian and other entities within Canada, where they are every day engaging with them in dialogue, responding to various disputes and forms of these conflict, do they have skills and tools to manage these encounters?

Bridging the Gap

Yet within this space, there may an opportunity to build resilience, defensive (and potentially even offensive) capabilities, through strategic conflict management considerations and effective negotiation practices. In my experience, working within both the security, defense, and intelligence community and now with law and corporate offices, and having worked in support of diplomats and politicians, I continue to see the absence of a strategic response to hybrid

warfare. Society has not yet absorbed that a significant majority of the threats and activities are outside the domain of government or military. The targets and responses are being managed quietly, often to mitigate reputational risk and embarrassment, and at times in real fear of the threat actors. However, with little attention so far focused on this domain, there seems to be a huge opportunity to mitigate and leverage both defensive and offensive opportunities, largely though not entirely through better negotiation and conflict management strategies.

The vast policy considerations appear all too obvious for a practitioner operating in this space, yet most suggested or obvious considerations have been either dismissed or given superficial consideration. To name a few obvious ones.

1) Legal Reform – specifically looking at the current legal impediments that prevent sharing of information between public and private sector, and equally between government departments? This includes reviewing the impact of the Charter of Right and how it through R v Stinchcombe and R v Jordan preclude sharing information amongst our international partners.
2) Public and Private Collaboration – in developing strategies, building leadership capacity on both sides, including working with Think Tanks and NGO's like Project Seshat that are offering our youth the who are attempting capacity in Universities and examining non-kinetic ways leaders in business, law, politics can contribute and play a meaningful role in combatting these threats, using more effective negotiations skills and strategies in their operations, including making the right decisions in their non-kinetic engagement with threat actors and their proxies in society.
3) Bolstering Our Education System – where youth, as like in Finland and other nations, children are taught about misinformation, fake news, disinformation vs the current curriculums that do not address these significant daily threats impacting Canadian society.
4) Intelligence Tools for the Private Sector – either build data banks or support "big data' with proper governance that allows Canadian society access to higher quality intelligence (via due diligence) to understand in their business, political and legal activities when they may be engaging with a potential high- risk transaction or engagement that may require altering their approach, including how they approach negotiation situations or resolve or avoid disputes with these entities. In many cases, AI, machine driven big data and other tools can assist the private sector navigate these threats and mitigate them. They are not always avoidable encounters and while the government spends massive amounts of funds for the "public sector" and rarely share, perhaps empower the private sector through

financing, research, governance, and regulation. As they say, non-shareable intelligence has little value and perhaps building the capacity in the private sector may prove more effective?

Perhaps through enhanced collaborative efforts of the military, intelligence, and policing, including formalizing a collaborative conflict management strategy that includes building negotiation capacity and supporting tools, such as artificial intelligence and public threat assessments, we can yet make progress in this area. I have personally witnessed lost opportunities, where law and business offices are perplexed and uncertain what the best course of action is, as they engage with the threat actors and situations of hybrid warfare. Yet all is not lost: this state of affairs is not necessarily permanent. The Chinese themselves have thoughtfully provided clues to effective responses, in one of their most ancient and widely quoted texts.

Sun Tzu's writings provide literally dozens of potential quotes relating to some of the issues, concerns and most importantly 'opportunities 'in enhancing a conflict management strategy, and developing enhanced negotiation approaches, in both a defensive and potentially offensive manner. An opportunity awaits those professionals engaged in defending democracies against hybrid warfare. There is an army of allies in the private sector: lawyers, business leaders, diplomats and politicians who are every day engaged in a quiet and discreet battle themselves, though currently often confused, perplexed and desperate for collaboration and partnerships. Should conflict management and negotiations be prioritized over other considerations? The answer is unknown. What is known is that it would be completely negligent to dismiss decades of research, practice and lessons learned in the area of conflict management and negotiations, including peacemaking, de-escalation, conflict mitigation—and the list goes on. Observing the response to the Huawei incident in Canada, seeing the non-strategic responses to cyber attacks, including business effectively funding state actors through ransom concessions, watching journalists and media companies flounder in lawsuits weaponized by China against Canadian journalists—and again, the list goes on. It's obvious there is no overall conflict management strategy yet, and those engaged in these non-kinetic disputes are getting crushed by our adversaries. After three (3) decades in the fields of both global security operations and conflict management, I am confident the lessons and strategies of conflict management and negotiations are not only largely absent in our responses, but perpetuate our failures in many instances.

The most obvious and pragmatic solutions include arming these current *first responders* not only with 'awareness 'of the gap, but more importantly with enhanced knowledge and capabilities in conflict management strategies, as they respond to the mergers, acquisitions and foreign influence activities in business, law, diplomacy, and politics. Equipping and arming them with the tools and support required to undertake their key roles in the defense of our country,

including sharing intelligence, but more importantly, building and sharing intelligence tools, big data, and artificial intelligence, will bolster our as well as their conflict management and negotiation effectiveness. Our adversaries have legislation that allows them to direct and deploy civilians in their national security initiatives. What is being suggested here is less ambitious and poses no risk to our cherished civil liberties: merely to support, equip and empower these sectors to defend and support themselves, and others with the same mission and concerns.

I leave the reader with Sun Tzu's famous quote, which parallels many of the concepts discussed in this paper: "When strong, avoid them. If of high morale, depress them. Seem humble, to fill them with conceit. If at ease, exhaust them. If united, separate them. Attack their weaknesses. Emerge to their surprise" (in Sawyer 1994).

Perhaps complementing the traditional military with contemporary conflict management strategies and alternative negotiation approaches, inclusive of the 'first responders', business leaders, legal professionals, diplomats, and political leaders, could be the X Factor. The X Factor in the spatial gap—which has not yet been fully examined or exploited by Western democracies as they 'mind the gap'. While Hybrid Warfare is different from Canada's peacekeeping missions in Cyprus, the former-Yugoslavia, Haiti etc., we were once known as one of the world's most formidable 'peacekeeping 'and equally important, 'peacemaking 'nations. It was one of our proudest traditions and accomplishments as a nation. This was achieved not by our kinetic capabilities alone, but rather by developing the ability of integrating kinetic capabilities with negotiation strategies in an approach which essentially was a 'conflict management ' approach to war. The world has evolved, and so has hybrid warfare. The battleground now is not only overseas, but encompasses our own communities within Canada. Key stakeholders include our business leaders, law firms and community leaders, all of whom are perplexed and confused by this new polarized and volatile setting; and in this new environment they are, perhaps, even more important as elements of our defence at times than the military and police.. Perhaps there is now an opportunity to revisit our 'peacemaking 'lessons learned, where 'conflict management 'practices brought Canada the highest respect amongst our allies, and revisit, modernize and include the private sector in the way forward, guided by an all-inclusive conflict management approach to hybrid warfare. Could this is even become the real X Factor?

References

BlackOps Partners. 2023. "Unrestricted Hybrid Warfare". *BlackOps Partners.* URL: https://blackopspartners.com/resources/.

Brown, M. 2022. "The Mind the Gap!". The *Londonist*. URL: https://londonist.com/london/transport/when-did-mind-the-gap-first-become-a-tube-thing.

Chrustie, C., J. S. Docherty, L. Lira, J. Mahuad, H. Gadlin, and C. 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.

Cristal, Moty. 2017. "Negotiating in a Low-Trust Environment". In *The Negotiator's Desk Reference*, edited by Chris Honeyman and Andrea Kupfer Schneider. St. Paul, MN: DRI Press.

Docherty, J. S., and C. 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, H., D. Matz, and C. 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.

Government of Canada. 1985. National Defense Act. URL: https://www.canada.ca/en/department-national-defence/corporate/reports-publications/transition-materials/defence-101/2020/03/defence-101/intro-nda.html.

Lira, Len. 2017. "The Military Learns to Negotiate – Chapter 74 *The Negotiator's Desk Reference*, edited by Chris Honeyman and Andrea Kupfer Schneider. St. Paul, MN: DRI Press.

Sawyer, Ralph D. 1994. *Sun Tzu -The Art of War*. London: Basic Books.

Wray, C. 2022. "Director's Remarks to Business Leaders in London". *FBI*. URL : https://www.fbi.gov/news/speeches/directors-remarks-to-business-leaders-in-london-070622.

How Hybrid Warfare is Redefining Contours of 'Business as Usual 'and the Potential Role of the Military

Anne Leslie

Introduction: How Hybrid Warfare Has Already Affected Big Businesses

Seemingly, not a week goes by without yet another big business falling foul of a cyber-attack, accompanied by a high-profile media outcry. Alarming (and sometimes alarmist) headlines point to the millions of confidential and sensitive data records that are now out 'in the wild 'as the result of continual data breaches. The victim companies and their executives are publicly chastised for sloppy cybersecurity practices, with accusations of professional negligence becoming increasingly prevalent.

We are seeing examples of individual Chief Information Security Officers bearing the brunt of responsibility for particularly serious incidents (such as in the case of the data breach at Capital One (Dark Reading, 2019) and similarly at Equifax (Fung, 2017). However, it is very infrequent that we see the media investigate the actual threat actors themselves to hold them to account for the execution of wholly reprehensible acts of cyber violence.

It is legitimate to question why this is the case. One plausible explanation is simply that it is much easier to blame the victims of cybercrime than it is to unravel an extremely complex and geopolitically charged web of interconnected organizations with difficult-to-discern motivations and relational ties that often lead back to nation-states operating in the so-called 'gray zone'.

Figure 1 - Unrestricted warfare in the gray zone via 'no rules' great power competition between nation-states (BlackOps Partners, 2022)

While reports of data breaches and cyber-attacks can become public very quickly—particularly when regulatory rules exist that require incident reporting above a particular impact threshold—the back story of what really happened and why can take years to come to light, if it ever does. And it is even rarer to see cyber-attacks in the private sector

publicly attributed to threat actors affiliated with nation-states, as the act of attribution is in itself a move of geopolitical significance that has ramifications extending far beyond the perimeter of the victim's organization.

There are numerous examples of companies all over the world that have suffered attacks on their IT infrastructure, and this article throws a spotlight onto three of the most high-profile cases. These examples effectively illustrate how enterprises are being compromised and manipulated as part of advanced, persistent threat campaigns, orchestrated at pace and scale by sophisticated adversaries including nation-states.

- The RSA breach (Greenberg, 2021): in March 2011, US-based security vendor RSA was the target of an attack that compromised sensitive data related to the company's flagship SecurID product. This software was in use by thousands of high-profile clients around the world, including the U.S. government and an array of U.S. defense contractors. A potent combination of low-tech social engineering and sophisticated malware that executed a zero-day vulnerability gave Chinese hackers nearly unlimited access to enterprise resources, costing the parent company of RSA (EMC) $66.3 million USD and exposing every one of SecurID's 25,000 customers to potential jeopardy.
- The NotPetya ransomware incident at Maersk (McQuade, 2018): a vulnerability in the tax return software used by the shipping and logistics giant allowed the NotPetya virus into the company's network, crippling it within minutes. While Ukraine was the primary target of NotPetya, in the context of an ongoing conflict with Russia, Maersk lost all end-user devices (The Economic Times, 2022) including 49,000 laptops and print

capability, with the subsequent financial loss estimated at approximately $300 million USD. This attack served as a wake-up call to business leaders globally that not all cyberattacks are targeted with precision. Organizations can find themselves the unintended victims of these incidents, incurring very significant operational, financial, and reputational loss in the process.

- The Solar Winds supply-chain attack (Williams, 2020): hackers targeted SolarWinds by deploying malicious code into its Orion IT monitoring and management software, used by thousands of enterprises and government agencies worldwide. The SolarWinds hack was a major incident not because a single company was breached, but because it triggered a much larger supply chain incident that affected thousands of organizations, including the U.S. government. The attack is generally attributed to the Russian Foreign Intelligence Service in the context of a Russian espionage operation, although suspected nation-state hackers based in China have also used SolarWinds in attacks.

While the threat of cyberattack is increasingly present in the minds of corporate leaders who fear the impact on their organizations from a financial, legal, and reputational perspective, the 'big picture 'view (illustrated in Figure 2) of how individual attacks may be part of an immensely broad, long-term, and programmatic campaign of attrition by sophisticated great power adversaries is unfortunately not a topic that often makes the agenda of company meetings.

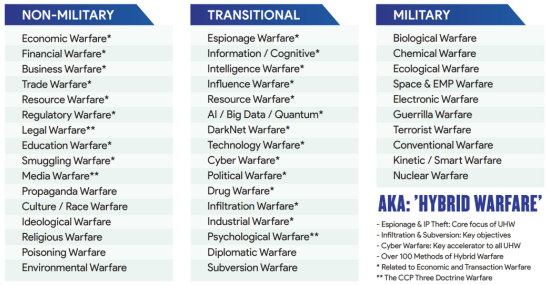


Figure 2 - The many dimensions of unrestricted hybrid warfare (BlackOps Partners,2022)

Therein lies a significant part of the challenge related to hybrid warfare, because without an appreciation at the decision-making layer of private and public sector organizations (outside of government, counterintelligence, defense and law enforcement) about how seemingly isolated cyber-attacks in the corporate sector may fit into an adversarial nation-state dynamic of hybrid asymmetrical conflict, the micro and macro level of preparation and response to the immediate and longer-term threats will continue to be ill-adjusted and inadequate.

How Can Canadian and Other Military Forces Help Businesses? And NGOs. And Municipalities. And….

The Role of Trust

A concerning observation about the nature of the relationship that currently exists between private sector companies and state-level bodies is that it tends to be characterized by a low level of trust (Edelmann, 2021), meaning that companies have a default posture

to disclose as little as possible and interact as infrequently as possible with these bodies.

While some jurisdictions, such as the European Union (EU), are using regulatory policy instruments (European Commission, 2022) to drive more cybersecurity discipline, capability-building, and accountability through potential enforcement actions, there is a case to be made for proportionally lighter-touch voluntary measures that aim to build cohesive information-sharing communities and joint coalitions between, for example, the military and civil society. As one US government official recently remarked in an industry roundtable, "Businesses and the public are our customers – it's on us to get our customers to trust us more. There are real adversaries out there trying to harm us; we need to get the public to stop seeing our own government as the enemy. We must put a foundation of trust in place, and fast!".

The military could participate in such initiatives through the creation of government-funded shared incident response capabilities that serve as public resources to enable cyber defenses on a whole-of-nation and cross-border basis. We can think of it in terms of creating a Cyber Defense Service akin to the Fire and Police Service, with trained military specialists whose role is to educate, build awareness, 'fire-fight 'locally on-site to respond to cyber incidents, and with a mandate to collaborate and police across borders to address the transnational nature of cyber-criminality.

Instead of expecting individual businesses and organizations to create, fund, train, and maintain their own cyber 'fire and policing service 'in-house – which is currently the de facto position for the small percentage of companies who have the financial means to pay for specialist services on retainer— there is a space for the military to take on the role of establishing and operating a set of protective, preventative, and responsive capabilities that would be publicly available to help civilian organizations prepare for and respond to cyber-attacks.

What we currently observe in the private sector is that cyber incident response capabilities sit in the hands of resource-rich and sophisticated organizations, which has the effect of leaving vast swathes of the economy and wider society unprotected. Furthermore, even when backed by the most mature capabilities, cyber incident response tends to be siloed by industry and technology vertical which means that it can only ever deliver a fragmented approach, opening up the risk of contagion from attacks as adversaries permeate the exposed adjacencies between companies, industry sectors, and countries.

Vertical cyber skill specialization by industry and technology is not per se a bad thing. It is indeed critical to match the sophistication of highly mature and organized adversaries. However, for maximum impact and to drive better defensive outcomes, these verticalized skills arguably need to be tightly aligned and loosely coupled with a new breed of publicly financed cyber incident response and threat intelligence capabilities. The aim would be to orchestrate a step-change in transnational collaboration between public and private sector cyber defenders, enabled by trusted cross-border information exchange, governance, and funding mechanisms to

counter the agile, jurisdiction-less nature of cybercrime through extended defensive geographical coverage and elastic resourcing to respond to attacks where they occur.

Such an approach would, at least in part, mitigate the existing fragmentation of response capabilities previously described, as well as create a locally accessible resource that brings skills, proximity, and cultural sensitivity, to address the more prosaic issue of "Who do I call?" when a cyberattack strikes in a business context and no retainer is in place to bring a squad of specialist incident responders on-site on an ad-hoc basis.

To address the foundational issue of trust, military forces would also need to engage in ongoing relationship-building, awareness, and outreach activities to ensure that the public knows that these cyber resources exist and that they will not be creating any additional risk of legal or reputational liability for themselves or their organizations by tapping into them and disclosing the occurrence of a cyber incident.

The challenge of funding, however, remains a complex hurdle to overcome. Immense personal conviction, persistence, and influence from emblematic public figures will be needed to drive a commitment across governments and agencies to articulate the case for a sustainable model of managing a global-local cyber defense commons as the lynchpin that secures our liberal democracies in the face of cyber adversaries who are determined to undermine them.

What Can Be Done with Cybersecurity Partnerships?

Cybersecurity is often framed as a 'data problem'. As practitioners, we are faced with a dual challenge. Firstly, the uncomfortable reality is that we often don't know what we don't know in the confines of our organizations, and this is exacerbated in the context of hybrid warfare. Furthermore, we suffer (paradoxically) from having an overabundance of data available to us, coupled with a paucity of actionable insight to steer decision-making and resource allocation.

A possible path forward to driving better micro and macro cybersecurity outcomes would be to leverage the economic principle of division of labor. In practice, this would translate to willfully driving specialization at different layers of society. Specifically, the military could specialize in providing threat intelligence and incident response capabilities to serve the real economy. In parallel, there would need to be actions undertaken elsewhere, to remove structural, cultural, and technical barriers to information exchange and collaboration, as a pathway to anchoring intentionally architected cyber interdependence between the public and private sectors, with the military playing a pivotal orchestration and technical enablement role.

The logic for such an approach is perhaps best explained through the example of threat hunting, which is the practice of proactively searching for cyber threats that are lurking undetected in a network. Threat-hunting is a sophisticated human-led activity, only practiced by a tiny minority of civilian

organizations due to the high level of organizational maturity and specialist expertise required.

As illustrated in Figure 3, even the most advanced civilian organizations are constrained in how far they can take their pre-emptive cybersecurity efforts because they lack the means to reliably establish the goals, strategy, and identity of the threat actors that may be targeting them.

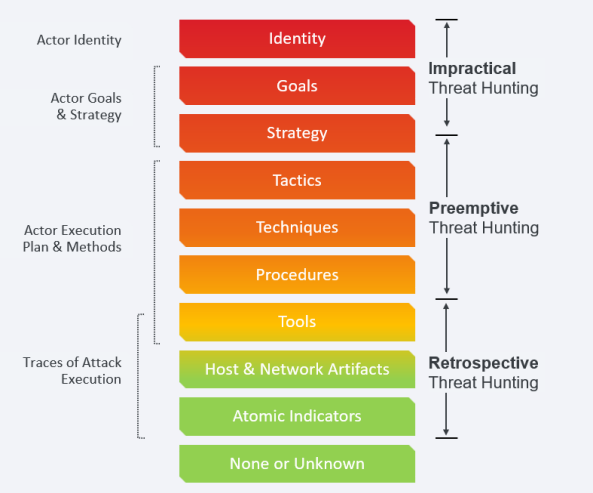


Figure 3 – Limitations of pre-emptive measures in civilian organizations (Bianco, 2014 IBM Security, 2019)

This is where trusted bilateral information exchange and collaboration between civilian organizations and military and intelligence agencies could prove invaluable. The military is arguably uniquely positioned to help organizations be more effective in their threat-hunting activities by mitigating the information asymmetry that currently hinders them. Similarly, the timely sharing of granular information originating in civilian organizations would allow the military and intelligence agencies to build a holistic and dynamic heat map comprised of weak signals and confirmed attacks, garnering a more accurate view of the preferred tactics, techniques, and procedures (TTPs) of different categories of threat actor, with an extension of the analysis into further categories of non-military gray zone conflict (BlackOps Partners 2022) (such as economic/financial/trade/resource/regulatory/ legal warfare) beyond the frontiers of what generally is thought of as a 'straightforward' cyber-attack, if such a thing exists at all.

Prevention and Its Roadblocks

Despite vast amounts of money being invested annually in cybersecurity, ($57.7 billion USD in 2021) (Statista, 2022) the outcomes delivered are objectively unsatisfactory.

A common shortcoming in corporate cybersecurity programs is a failure to take a dynamic, systemic view of the overall attack surface (including the digital supply chain) which leads to organizational blind spots and a false sense of certainty. This is frequently further compounded by a failure at the executive level to unite strategy, technology, risk, security, and the human factor into a cohesive, enterprise-wide protective motion.

As the NotPetya attack at Maersk shows, one of the key lessons is that businesses would be naïve to approach their cyber defenses with the assumption that their defenses need only to focus on attacks will specifically target them. The evidence shows that businesses can all too easily find themselves being collateral damage in a much wider inter-state conflict to which they likely do not even consider themselves a party.

While there is undoubtedly merit in instigating more cybersecurity-oriented collaboration between businesses and the military, this should be positioned as an enabler and amplifier of the individual preventative, protective, and recovery measures that remain within the locus of control of individual organizations.

Business leaders and their Boards must assume accountability for ensuring the company knows in detail all their core business processes, systems, and applications and then consistently tests their preventative and recovery capabilities against a set of plausible-but-severe scenarios that are threat-informed and risk-based, so that in the event of an attack occurring, the business has demonstrated operational resilience enabling it to operate even in the event of extreme disruption.

To drive progress in effectively thwarting cyber-attacks 'left of boom 'and mitigating the impact 'right of boom '(military parlance for describing the timeline of events before and after an explosion or incident), it is incumbent upon us all – corporations, NGOs, universities, government agencies, policymakers, law enforcement, and the media – to intentionally move beyond a culture of sensationalist victim-blaming, a defensive limitation-of-liability mindset, and siloed actions into a far more helpful posture of radical curiosity, open collaboration, and pragmatic capability-building.

Today, a corrosive combination of complacency, inertia, and fear is inhibiting organizations in the exercise of their individual agency to drive more effective cyber-defense programs. Between a lack of awareness and a lack of willingness lie myriad believable but spurious reasons for businesses not making a move to improve their cyber hygiene and overall security posture.

At the same time and depending on the particular jurisdiction and the size and systemic relevance of a given organization, policymakers are now leveraging a variety of methods to induce behavioral change.

In the United States, for example, the Cybersecurity and Infrastructure Security Agency (CISA) recently published a set of cybersecurity performance goals (CISA, 2022) to help critical infrastructure operators and other companies prioritize the adoption of key security measures. The goals represent a minimum baseline of cybersecurity measures that organizations can adopt on a voluntary basis to ensure the resilience of their systems and drive down risk. If implemented, these measures aim to reduce not only risk to critical infrastructure, but also to national security, economic security, and public health and safety.

As we move forward as professionals in our organizations and as citizens in our societies, we need to push ourselves to better understand the forces at play below the surface of our daily activities and in our periphery, challenging ourselves to reflect critically about what we think we know for certain. We need to be inquisitive about how disparate incidents and seemingly random attacks may potentially connect to each other and to a more encompassing, concerted adversarial strategy of destabilization. Most critically, we need to acknowledge that tackling the issue of cybersecurity in the context of grey-zone

conflict is more than any single organization can take on.

Conclusion

Impactful cybersecurity practices require orchestrated and outcome-oriented contributions from individual organizations across all layers of society, accompanied by whole-of-nation enablement and coordination at the level of government and the military that extends across geographical borders to include likeminded, trusted partners in the private and public sectors.

For such a model to materialize, the role of the military as a benevolent, trusted cyber force at the service of commercial entities and the public needs to evolve. In the absence of this essential foundation of trust, the real adversaries will continue to reap the rewards of the endemic ambivalence we currently have towards each other in our democracies, with the ensuing division and fragmentation creating a ripe playground for ongoing non-kinetic acts of destruction and destabilization.

References

Bianco, D. 2014. "The Pyramid of Pain". *SANS*. Extrapolated from the original work by IBM Security.URL: https://www.sans.org/tools/the-pyramid-of-pain/.

BlackOps Partners. 2022. "The Gray Zone." *BlackOps Partners*. URL: https://blackopspartners.com/wp-content/uploads/GrayZoneC.pdf.

BlackOps Partners. 2022. "The Modern Battlefield is Everywhere." *BlackOps Partners.* URL: https://blackopspartners.com/wp-content/uploads/Unrestricted-Warfare.pdf.

CISA. 2022. "Cross-Sector Cybersecurity Performance Goals." *CISA*. URL : https://www.cisa.gov/cpg.

Dark Reading Staff. 2019. "Capital One Shifts Its CISO to New Role". *Dark Reading*. URL: https://www.darkreading.com/risk/capital-one-shifts-its-ciso-to-new-role.

Edelman. 2021. "Country Report: Trust in Canada." *Edelman*. URL: https://www.edelman.ca/sites/g/files/aatuss376/files/trustbarometer/2021%20Canadian%20Edelman%20Trust%20Barometer_0.pdf.

European Commission. 2022. EU Cyber Resilience Act. *European Commission.* URL *:* https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

Fung, B. 2017. "Equifax's security chief had some big problems. Being a music major wasn't one of them." *Washington Post*. URL: https://www.washingtonpost.com/news/the-switch/wp/2017/09/19/equifaxs-top-security-exec-made-some-big-mistakes-studying-music-wasnt-one-of-them/.

Greenberg, A.. 2021. "The Full Story of the Stunning RSA Hack Can Finally Be Told." *Wired*. URL: https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/.

McQuade, M. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*. URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Merchant, Z. 2022. "NotPetya: the cyberattack that shook the world". *The Economic Times of India.* URL: https://economictimes.indiatimes.com/tech/newsletters/ettech-unwrapped/notpetya-the-cyberattack-that-shook-the-world/articleshow/89997076.cms?from=mdr.

Statista. 2022. "Spending on Cybersecurity Worldwide from 2017 to 2022." *Statista.* URL: https://www.statista.com/statistics/991304/worldwide-cyersecurity-spending/.

Williams, J. 2020. "What You Need to Know About the SolarWinds Supply-Chain Attack". *SANS*. URL: https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/.

Hybrid Warfare – Is it New, is it Real, and What are the Threats, Vulnerabilities, and Implications for Defence and the Military?

Steven Desjardins

Introduction: Neither "War" nor "Peace"

The following article is intended to provide a general overview of the increasingly complex, ambiguous, and dangerous nature of the security environment. Beyond the doctrinal debates on hybrid/grey zone warfare, the reality is that making a clear demarcation between war and peace, public and private can no longer drive national security or private security policies as competitors have increasing ease, utility, persistence and reach in exploiting all levers of national power to achieve their national objectives. Hard power or kinetic means are no longer the pre-eminent means for imposing an entity's will on an adversary.

This article is complemented by the On Track articles "Mind the Hybrid Warfare Gap" (Calvin Chrustie); "How Hybrid warfare is Redefining the contours of "business as Usual" and the Potential Role of the Military" (Anne Leslie); "Working Across Silos" (Chris Honeyman); and Hyrbrid Warfare: Fighting Back with Whole of Society Tactics" (Sandra Jaufman) where greater details are provided on threat and hostile activities as well as with regards to policy implications.

Historically there is a tendency to view the security environment in binary terms—"war and peace"—and to view defence and security challenges through lenses of new forms of "warfare" or revolutions in "military" affairs. Some analysts, scholars and practitioners argue that hybrid represents a new evolution in warfare. Others are equally convinced that hybrid warfare, or as the Americans now refer to it, "Gray Zone Warfare," represents nothing new aside from changing terminology (e.g. irregular warfare, unrestricted warfare, asymmetric warfare, compound warfare, 4th Generation Warfare, the indirect approach, compound warfare, low intensity warfare" (Horn, 2016)).

However, as Dr. Emily Spencer has argued, "Redefining a problem because you cannot find a solution that is palatable does not actually change the circumstances; rather, it simply perverts your point of view." (Spencer 2014, 66). And as Arthur de Liedekerke and Maarten Toelen have observed, "In keeping with Clausewitz's theory, hybrid war can be conceptualized as a coordinated and synchronized application of force below the accepted but outdated thresholds of traditional war, seemingly defined by human casualties or

material damage, by employing a wide range of military and non-military instruments to achieve political objectives, most notably through the instrumentalization of cyberspace as an instrument of warfare" (de Liedekerke & Toelen 2022).

Much of what we now experience and refer to as hybrid warfare has been and remains an integral part of the fabric of inter-state competition and warfare. Hostile actors strive to change the global order of things without provoking open kinetic hostilities. As the UK Chief of Defence Intelligence put it "Whilst conventional threats remain, we have seen our adversaries invest in Artificial Intelligence, machine learning and other ground-breaking technologies, whilst also supercharging more traditional techniques of influence and leverage" (United Kingdom, 2020). Figure 1 illustrates the space most active to generate this competition below the threshold of war:

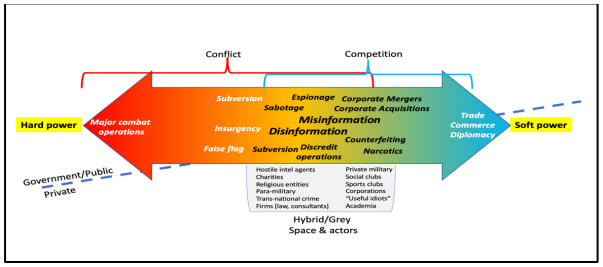


Figure 1: conflict and competition spectrum and the hybrid space (from the author)

Leveraging all forms of national power, in a coordinated and synchronized manner, is not new. Mixing and matching elements of national power to deceive, deny, delay, destroy and disrupt an adversary is not new. The substantive changes we experience in today's security environment are economic globalization, changes in the information environment [5], increased societal interfaces and emerging technologies. These have very substantively amplified whole new realms of societal vulnerabilities to hybrid threats, and they have very substantively empowered and facilitated access to hybrid means for hostile state and non-state actors to employ to generate ambiguity and achieve strategic, operational, and tactical effects.

Figure 2 illustrates the changes in how power is applied:

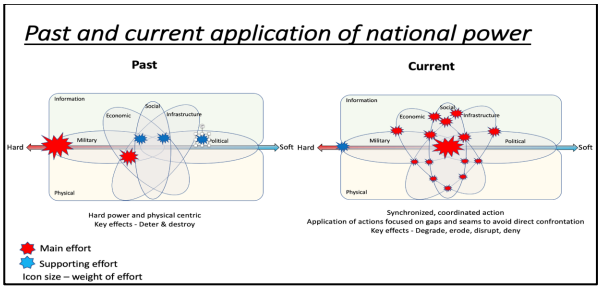


Figure 2: Illustrative shift in the application of national power (from the author)

As a result of the changes noted above, as illustrated in figure 2, the mixing and matching, coordinating and synchronizing of conventional and unconventional elements of national power, along with leveraging ambiguity in targeting these against societal interfaces to defeat, disrupt, deny or degrade an opponent's decision-making processes and ability to act, is more accessible than previously. It is also executed with much

[5] Ubiquitous computational power, exponential growth in the volume of information, exponential acceleration in the velocity at which information moves and the democratization of information are all significant changes.

greater speed, reach, depth and persistence, and this "pays dividends despite being easier, cheaper, and less risky than kinetic operations.

Figure 3 illustrates how an adversary can alternate in intensifying some levers, and reducing others, to generate ambiguity, achieving the desired effect while remaining below the threshold of war:

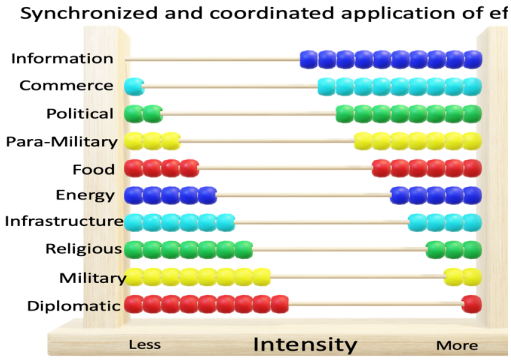


Figure 3: Synchronization, coordination of the ways, and means (from the author)

The Dominant Active Hybrid Warfare Players

In the paragraphs above, the focus was on the what and the how actors are able and enabled to exercise greater reach, persistence in delivering effects while, by generating ambiguity, anonymity, they disrupt friendly actors from understanding or countering said hostile actions. The next portion will explore some of the more active and/or dangerous actors who currently exploit hybrid actions These actors fall into several categories as follows:

- State(s) on State; (the focus of the narrative below);
- States on Non-State entities, with the usual intent of coopting and reprogramming;
- States through non-state actors, often a form of classic insurgencies through means other than war, to include leveraging contracted actors (private military corporations, hackers, social media exploitation); and
- States through non-state actors on non-state organizations to coopt, exploit peer to peer relations (i.e. leveraging academia, the arts, media, sporting, charities…).

China, Russia, Iran and North Korea are the more notorious and well-known actors involved in hybrid warfare, all aspiring to "take on capitalist democracies and hoping to re-make the international political, economic and trade systems" (Strategy Vision, 2021). All seek to achieve this through actions that remain below the threshold of war, or at a minimum, actions that delay the onset of military kinetic actions. In terms of their capacity, sophistication, breadth, and impact of their ongoing campaigns, while North Korea and Iran generate ripples, and while Russia generates waves, China drives the tide. The remainder of this paper will therefore focus on China.

"China's People's Liberation Army first openly advocated the benefits of a hybrid approach in its 1999 publication *Unrestricted Warfare* which proposes avoiding democracies 'strengths and instead targeting

areas such as reliance on technology and respect for the rule of Law" (ibid).

Although military power will always have a role as target of or a means for generating strategic effects, "the erosion of economic strength is probably the most important element to target, with the broadest impact and the hardest to reverse. The key targets in the effort are businesses" (ibid). China's ability to exercise full or partial control over segments of the supply chain not only degrades a target state's economic power but also sets conditions for China to deny, disrupt or degrade the timely and effective generation of military responses, should those be necessary. China's military-centric "unrestricted warfare" framework rapidly and aggressively expanded beyond the military domain to become a Whole of Society effort, all aimed at securing the regime and elevating China to becoming a great power.

In the economic and business sector, Chinese overt and clandestine acquisition of foreign national infrastructure in Asia, Africa, Europe [6] and Canada, and the discreet acquisition of energy, agriculture[7] and mining sectors[8], particularly in rare earth minerals[9], are increasingly well understood and cause for alarm. At the same time, by the end of 2020 a total of 1,040,480 foreign companies were registered in Mainland China, according to official data provided by the Ministry of Commerce (MOFCOM).. All of these, naturally, are particularly vulnerable to a variety of Chinese tactics for influencing or infiltrating Western firms.

While leveraging economic means is currently a dominant approach, it is not the exclusive tool. Enabled by its political structure and political culture, the Chinese regime is capable of, and is, leveraging "a comprehensive portfolio of legal, semi-legal and illegal operations. They are overt as well as clandestine and implemented by CCP organizations, front organizations specifically launched for such purposes, or the employment of recruited "useful idiots". They include disinformation and manipulation, discrediting, counterfeiting and sabotage as well as destabilizing foreign governments, provocations" (Stumbaum 2022).

China has likewise leveraged military means, as in the episodic military embargoes and exercises aimed at keeping Taiwan in a box. China has infiltrated academia and both public and private R&D (Montreal Gazette 2022) to maintain its edge in emerging technologies, it is reputed to be involved in illicit drug production (Felbab-Brown, 2022) and distribution to undermine and impose

[6] 20 European countries are now part of the Belt and Road initiative. For example, China is financing the expansion of the port of Piraeus in Greece and is building roads and railways in Serbia, Montenegro, Bosnia-Herzegovina and North Macedonia (BBC 2019).

[7] In 2015, a special investigator was hired to probe "rumors that certain interests are trying to get around our law... that these people (buyers) are funded by offshore money," as well as "where the investment money is coming from." (Fox News, 2015).

[8] For the past two decades, China has built up a powerful position in Canada's critical minerals and mining sector, with little oversight from Ottawa (McGee, 2022).

[9] China controls about 90 percent of the global trade in rare earth minerals. Because production of rare earth minerals is a national security issue, dependency on REM poses a threat to our military capabilities (Chang 2022).

economic burdens on Western society, it has deployed security services abroad to monitor and control its expat population, and it has expanded its ability to influence foreign states through donations to opposition movements. In the end, China has positioned itself well to influence, degrade, deny, and disrupt multiple segments of Western decision-making and Western nations 'ability to act.

The Employment of the Military in a Security Environment Characterized by Hybrid Warfare

Thriving in a security environment characterized by hybrid warfare rests on a state's ability to achieve decision advantage and freedom to act. This rests on:

- achieving a "whole of society", or, short of this, a minimum "whole of government" shared comprehension of the threats and the risks, and establishing a shared threshold for risk across the nation; and
- public confidence and trust in the state's institutions.

Achieving a "whole of government shared comprehension" rests on nesting military power within a cohesive and integrated national framework. If hybrid warfare actors exploit the gaps that exist at the interfaces, then "closing the seams" between these societal interfaces is key. Only a unifying strategy can set conditions for this to be achieved.

The starting point is the creation of a unifying national security strategy that contributes to creating whole of government cohesion in *perceiving*, *making sense of*, and *acting to counter* hybrid threats. In turn, the national security strategy informs and drives the development of a defence strategy which sets the focus and aperture for generating, within a whole of government framework, the necessary defence effects.

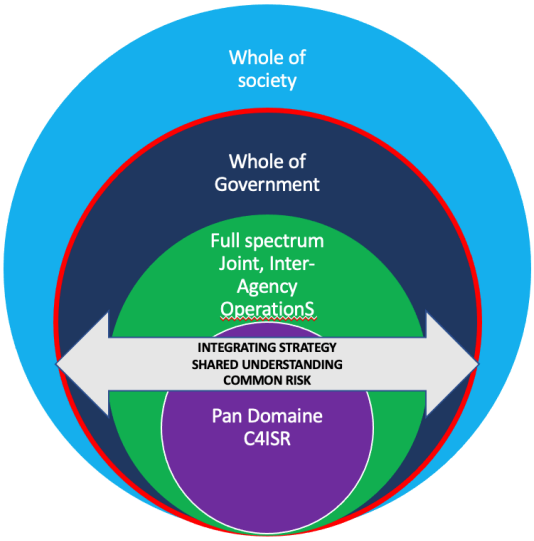


Figure 4: Integration of functions from military to whole of society (from the author)

Internal to the military itself is its key role in contributing to national resilience, and to detecting and generating a whole of society (ideally) or whole of government understanding of hybrid warfare threat activities.

On the former, a critical element is that of ensuring that the military and defence do not themselves become a liability. Closing the seams between operating domain interfaces (maritime, land, air, space, cyber, informational) is key to this. Institutionalizing and operationalizing pan-domain command & control, intelligence, surveillance and

reconnaissance is critical to both informing a whole of government understanding of threats, risks and opportunities and ensuring that the military does not constitute a liability to the nation.

Additionally, enhancing the military's ability to collaborate, operate and share with other government departments and agencies, as well as with non-traditional partners, is another means for minimizing gaps and seams while empowering whole of government actions in a hybrid environment. This is especially pertinent to defence intelligence, where operating with traditional and non-traditional government and civilian partners enhances the insight generated by inter-agency intelligence capabilities.

Cultivating closer relationships with the private sector is another way of minimizing military and by extension whole of government vulnerabilities, particularly emerging ones resulting from the military's ingestion of increasingly complex and complicated technologies produced by industry. Establishing and cultivating enduring relationships between the military and the private sector will contribute to enhancing the mutual understanding of risk, enhance operational security, and build confidence in the employment of technologies necessary to operate in the contemporary security environment.

As for the actual employment of the military within a hybrid context, the traditional warfighting role remains critical. Maintaining the ability and intent to deter and destroy will always be necessary to contributing to a state's national security. In addition to this primary function, more effectively leveraging the military's global intelligence collection capabilities, to include Defence Attaches etc., is increasingly important. With a global footprint of domestic and allied nations, the military is well positioned to contribute to perceiving, making sense of and addressing hybrid threat activities as they emerge.

Public Confidence and Whole of Government Freedom of Manoeuvre.

A well developed and operationalized hierarchy of strategies, from a national security to defence to military strategy, is essential. Employing a military force which has minimized its internal vulnerabilities and contributes to detecting and recognizing threats beyond its traditional focus is likewise key. However, to ensure all the above is achievable, more is necessary. The "information, cognitive and social domains becoming the cornerstone of hybrid warfare, any set of solutions sans confidence-and trust-building will probably fall short of offering effective antidotes" (Bilal 2021).

The public is a critical vulnerability in hybrid warfare. Undermining national power by eroding public confidence in national institutions or critical infrastructure is omnipresent in the contemporary security environment. "Contemporary digital and social media platforms allow hybrid actors to influence this to the detriment of the adversary state with considerable ease" (ibid). Maintaining public confidence in state institutions and trust between state institutions is vital to empowering said institutions with the authority and abilities to act at the speed of

strategic and operational relevance. If this is achieved "then society will become more resilient (Strategy Vision 2021).

Maturing a true national security culture and establishing trusted mechanisms for ensuring that the public has insights into its intelligence and security entities contributes to enabling strategic freedom of manoeuvre. In Canada, the National Security and Intelligence Committee of Parliamentarians (NSICOP) is a nascent parliamentary forum which, in spite of its infancy, has much potential for generating the transparency necessary to cultivating public confidence, and by extension, in maturing a national security culture and enabling government freedom to act and defeat hybrid warfare threats.

Additional Considerations for the Employment and Contribution of the Military

In addition to the above, there are several advances in the military's ability to operate in the information environment that, if shared with other government departments, would assist in de-risking the nation vis-à-vis hybrid threats. Evolving tools like Command and Control in the information environment (C2IE) by more fully leveraging artificial intelligence, machine learning and human-machine teaming will accelerate the military's ability to detect, recognize and understand activities that would otherwise go unrecognized. Furthermore, sharing these critical enablers across government would contribute to achieving a more comprehensive and shared understanding of the situation and risks across all societal interfaces.

Finally, the professional education curriculum applied to military and defence personnel could be expanded and broadened to include more public sector personnel, and potentially, private sector players as well. Education as a means for closing the gaps between government and other public-sector as well as private-sector entities would minimize vulnerabilities and achieve a broader understanding of risks.

Conclusion

In the end, whether hybrid warfare is a new phenomenon or not, the fact remains that exploiting all levers of national power to achieve strategic ends is not new. What has changed is the exponential growth in societal interfaces that constitute key vulnerabilities exploited by hostile nations to wage hybrid warfare, as well as the ambiguity, speed, breadth, persistence and reach now afforded to hostile actors. In particular, hybrid warfare can be increasingly effective by using emerging technologies and the evolution of the information environment.

Finally, waging war through hybrid means is more efficient and lower risk than warfare through conventional means. Combating this effectively is now a necessity for all parts of society. But only a national government has the means to coordinate other sectors, to remove roadblocks to civil-military cooperation, and to marshal the necessary resources. As the entities within government with the most relevant expertise and the best existing resources, the military and the defence ministries must assume central roles in this societal shift.

References

BBC. 2019. "How much of Europe does China Own?" *BBC News*. URL: https://www.bbc.com/news/world-47886902.

Bilal, A. 2021. Hybrid Warfare – New Threats, Complexity, and 'Trust 'as the Antidote." *NATO Review.* URL: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.

Chang, F. 2022. "China's Rare Earth Metals Consolidation and Market Power." *The Foreign Policy Research Institute.* URL: https://www.fpri.org/article/2022/03/chinas-rare-earth-metals-consolidation-and-market-power/.

de Liedekerke A. & M. Toelen. 2022. "The Relevance of Clausewitzian Theory in Hybrid War: The Iranian-Saudi Rivalry." *Hybrid CE Working Paper*. No. 15. March 2022. URL: https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220324_Hybrid_CE_Working_Paper_15_Clausewitz_WEB.pdf.

Felbab-Brown. 2022. "China and Synthetic Drugs Control: Fentanyl, Methamphetamines, and Precursors." *Brookings*. URL: https://www.brookings.edu/research/china-and-synthetic-drugs-control-fentanyl-methamphetamines-and-precursors/.

Fox News. 2015. "Chinese Buy up Canada Farms; is Beijing Behind it?". *Fox News.* URL: https://www.foxnews.com/world/chinese-buy-up-canada-farms-is-beijing-behind-it.

Horn, B. 2016. "On Hybrid Warfare". *CANSOFCOM. URL:* https://publications.gc.ca/collections/collection_2017/mdn-dnd/D4-10-19-2016-eng.pdf.

McGee, N. 2022. "China has Encroached on Canada's Critical Minerals Industry, with Almost no Obstruction from Ottawa". *The Globe and Mail.* URL: https://www.theglobeandmail.com/business/article-chinese-business-buying-canadian-critical-mineral-mines/.

Montreal Gazette. 2022. "Alleged Chinese Spy at Hydro-Québec Formally Charged, Considered Flight Risk." *Montreal Gazette.* URL: https://montrealgazette.com/news/local-news/alleged-chinese-spy-at-hydro-quebec-formally-charged-considered-flight-risk.

Spencer, E. 2014. "Back to Basics: Old School Rules." In Dr. Emily Spencer, ed., *By, With, Through: A SOF Global Engagement Strategy*. Kington: CDA Press.

Stumbaum. M.B. 2022. "China's Power Politics 2.0: Regime Survival and Global Leadership". *Hybrid COE Trend Report. No. 8.* URL: https://www.hybridcoe.fi/wp-content/uploads/2022/04/20220421-Hybrid-CoE-Trend-Report-8-Chinas-power-politics-20-WEB.pdf.

Strategy Vision. 2021. "Hybrid Warfare: the New Face of Global Competition." *Strategy Vision*. URL: https://strategyvision.org/en/news/34/--hybrid-warfare--the-new-face-of-global-competition-.

United Kingdom. 2020 "Chief of Defence Intelligence Comments on Threats the UK will Face in Coming Decades". URL: https://www.gov.uk/government/news/chief-of-defence-intelligence-comments-on-threats-the-uk-will-face-in-coming-decades.

How Should the Whole-of-Society Respond to Hybrid Warfare?

Sanda Kaufman

My contribution to the study of Hybrid Warfare (HW), rooted in a public policy perspective, focuses on how members of open societies such as Canada and the United States experience HW attacks, and on who can/should do what to improve preparedness and responses. Thus, I speak for, and to the direct and indirect victims of HW, and reflect on how they might be persuaded to get informed and care about HW consequences and devote resources to countering them.

I begin by identifying some obstacles to the public's recognition of HW. Then I argue that we can draw on other public policy challenges, such as disaster preparedness, to learn about possible strategies to mitigate HW damage, and about difficulties in implementing these strategies. I describe an approach designed for peacebuilding (Burgess & Burgess 2020) and for reducing societal polarization (Burgess et al. 2022) and propose that public and private organizations and individuals can adopt this approach to respond to HW.

Obstacles to Recognizing HW

HW may seem new, but perhaps it is not if we think of it as an updated version of the notion that "the end justifies the means." In fact, countries, groups, and organizations have always used deceptive, covert methods to complement visible, brute force attacks on their enemies. Both Sun Tzu in his "Art of War" (around the 5th century BCE, perhaps the oldest military treatise in the world, De Cock 1998) and Machiavelli (Reiley 2008) theorized that deviousness, deception, and fraud are legitimate and even necessary in the pursuit of (military, national) goals.

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 or drones), using information—correct or not—to target and rally various groups unaware of the real intent (e.g., youth recently destroying culturally valuable objects as a means of fighting against climate change), dividing and weakening various opponent groups (e.g., polarizing parts of societies to impede joint decisions, Burgess et al. 2022), and reaching out to the very young to addict them to social media activities and ideas that brainwash, or even to drugs.

Conducting HW against Western democracies is helped by their open, porous physical and social structures. Vital physical networks remain largely unprotected and insufficiently resilient even after repeated HW attacks. For instance, in 2003 a single failed power line in Ohio triggered a cascade of events, causing a major power outage which

affected about 50 million people, infrastructure systems, and public health in the Midwest and Northeast US and parts of Canada (Kile et al. 2004). It uncovered critical vulnerabilities which could still be relatively easily exploited, especially since they have yet to be remedied (Biello 2013). Awareness of HW threats and knowledge of how to protect vital infrastructure do not yet amount to action by either governments, private organizations, communities, or individuals.

In the social realm, the young (and their parents[10]) seem largely unconcerned by loss of privacy through interaction with social networks. Some are oblivious to the perils of having personal information—location, health data, statements on social media—collected and stored ostensibly for commercial and political purposes but potentially also for HW actions. Others consider that data privacy no longer exists, and therefore efforts to protect it are unwarranted or futile. They tend to see no downside, and readily believe that the perils amount to conspiracy theories—a term much in use currently and applied broadly to information that diverges from entrenched perceptions. That unfriendly entities might conduct surveillance and store personal data at a massive scale appears to many far-fetched.

Nevertheless, some perils of such individual data collection efforts through social media have been recognized. For example, the United States is considering shutting down the (Chinese-owned) TikTok platform [11] at least on public agencies' equipment. Twenty-six US states have already done so. There is concern with both the information TikTok disseminates, and with the extensive personal data collection in which it engages (Tyagi 2022). Awareness is also increasing about the devastating effects of readily available opioids in shapes and colors designed to attract children, and about the sharp increase in accidental deaths they are causing in Canada and in the US. These might be unrelated activities, just as they might be components of an as yet unrecognized strategy to undermine Western countries through multiple avenues.

The complexity of our intertwined social, economic, and physical systems (e.g., Kaufman et al. 2022) both internally and between Canada and the US contributes to the difficulty individuals and organizations have in recognizing HW moves and linking them to outcomes. For example, three seemingly unrelated events occurred within a couple of days in summer 2022 in Canada: Rogers, Netflix, and Twitter briefly went off-line in quick succession. This could have been a random coincidence, just as it could have been a nefarious test of how Canadians and their government react to loss of their communication and entertainment channels. The inability to unequivocally link causes to effects characterizes complex systems and

[10] However, in 2015 Dugan et al. (Pew Research Center) found that 33% of parents24 said they have had concerns or questions about their child's technology use in the past 12 months. The survey also found that most respondents "*have felt uncomfortable about the information posted about their child by others online"* but that "*few have requested content be removed.*"

[11] According to Vogel et al (2022), "*TikTok has established itself as one of the top online platforms for U.S. teens."*

provides a space for HW actors to inflict unimpeded damage, unless we—individuals, institutions, and countries—organize to protect ourselves.

But who is "we?" In HW matters, as in warfare by any other means, it is necessary to establish who "we" are, for whom "we" speak, and whom we are helping to protect. HW response strategies hinge on this recognition and require taking sides and considering ours to be worth defending. This has become rather difficult in the 21st century, as some societies—ours included—question their values and past actions, while those conducting HW have no such qualms.

A basic asymmetry exists between open societies, such as Canada, and the United States, and aggressive dictatorships. Open, wealthy societies tend to be risk-averse to military confrontations and the ensuing losses. They operate more or less transparently, sometimes even announcing to adversaries how they plan to respond to their attacks, as well as what they will not do. They mostly expect to negotiate with (identifiable) opponents when conflicts arise. However, these open societies are increasingly divided internally, perhaps partly for lack of a perceived common enemy that rallied them in the past. Internal divisions sometimes prevent democratic societies from engaging in actions they deem necessary, but which fail to garner broad public consensus.

In contrast, dictators act aggressively—think leaders of China, North Korea, Russia, or Iran—being unconstrained by their subjects 'wishes or positions. Instead, they seek to focus their publics 'attention on external threats and away from internal problems imputable to the leaders. Therefore, where an open society might wish to engage in negotiations to manage conflicts, dictators may reach for HW means to achieve their goals, chief among which are remaining in power, and extending this power beyond their borders in time and space. Their acts of HW aggression may require HW responses along with other defense measures.

An added obstacle to recognizing and responding effectively to HW is a differential attitude to time. Developed countries treat time as a commodity in short supply. They tend to have a short horizon for decisions and actions, driven by election cycles that occur every 2-5 years. Most other cultures and countries are patient in the pursuit of objectives, not least because dictators at their helm stay in power for extended periods. Their long horizon—lasting even decades—allows them to slowly prepare the terrain for surreptitious takeovers, using HW moves that remain unrecognized or are considered benign until they percolate through entire countries to damage target societies. These moves include purchasing valuable or strategically positioned assets and land in their targets 'midst, disguised as normal transactions that seem economically advantageous to local populations in the short run; slowly acquiring resources and production means predicted to become scarce and central to the functioning of key technologies on which the economies already rely or will increasingly do so in the future—such as rare metals for electric car batteries or solar panels; and developing and testing technologies which can destabilize infrastructure for key societal needs—

electricity, clean water, transportation, hospitals, communications. Examples of such attempts abound both in Canada and the US, though we may not have developed yet the means to recognize them as concerted HW and to respond effectively or even preempt them.

Protecting against HW – What can Canada and the US Learn from How Governments and the Public Respond to Other Threats?

HW uses novel technologies, an element of surprise, and is waged at different scales, from local to country-wide. Defensive action may have to include similar technologies and tactics in TIT-FOR-TAT manner,[12] to signal to opponents that their moves have been recognized as hostile,[13] and to increase the costs of their HW use and even deter them. However, individuals and organizations are unlikely to have their own HW capability to counterattack HW effectively. They may, however, learn to recognize, prepare, and defend against HW, by borrowing from other domains.

In complex, networked social systems such as ours, individuals, and public and private entities at all scales can self-organize against shared threats such as HW—if they see the need for it. HW is not unlike natural hazards in that vital systems can be disrupted with no warning. Those who take the time to imagine what they will need in order to recover effectively from a disaster—or an HW attack--and then put it in place, will fare better than those who are unprepared (Shmueli et al. 2021).

Disaster preparedness faces similar obstacles to HW: lack of awareness and lack of willingness to devote resources to mitigate consequences of sudden events such as hurricanes, (even when frequent and expected), earthquakes, or slow-unfolding events over the long term such as climate change (Shmueli et al. 2021). HW may be unfolding slowly, but also consists of sudden, unexpected hits—some designed to learn how their targets respond, to better defeat them at the next round. What can we do to protect ourselves and our societies from HW damage? And who should do it? First, I will discuss some obstacles to effective HW responses, and then some possibilities for action.

In my planning and public policy experience, persuading people and politicians to act, whether to counter HW or prepare responses to natural hazards, is very difficult: these challenges lack salience (in other words, "perceived immediacy") and reacting to them is costly. HW requires continual vigilance in the moment, as well as long-term plans. In that sense, preparing for HW encounters similar obstacles as fighting climate change (CC). Both tend to be perceived as either not real, out of sight/out of mind, or too advanced to oppose successfully.

People's immediate concerns take precedence over long-term threats. Politicians do not like to devote effort and resources to

[12] TIT-FOR-TAT is a strategy that is successful in repeated Prisoners' Dilemma games (Axelrod 1980) and consists of responding by cooperating or competing at each turn as the opponent did at the previous turn.

[13] A technique negotiators call "naming it" to make counterparts aware that their underhanded strategies have been recognized.

problems if they won't get credit for success in time for elections. For example, the extensive preparedness to the Y2K threats to computer technologies and consequently to global economies averted the predicted catastrophes. However, it is still considered an over-hyped problem on which government and private resources were wasted, since what so many feared did not happen. Of course, this may have been precisely *because of* the resources and efforts devoted to preparations.

In contrast to Y2K, which was socially amplified to the public (MacGregor, 2003), vital infrastructure in the US is neglected because investments have no immediately visible benefits that might help re-elect politicians operating with 2- or 4-year horizons. The public only becomes aware of the neglect when accidents occur, such as crumbling bridges or disruption of the drinking water supplies, as happened in Jackson, Mississippi (Ko 2021). Fixing Jackson's drinking water shortages is predicted to take the next ten years.

Getting people to attend to rare but very destructive earthquakes, such as the one expected along the San Andreas fault in the Western US, is also uphill. Borrowing from Taleb's (2007) label for surprising, never-seen-before events, I call 100-year earthquakes and floods *generational black swans.* Though not unique, they are new to each generation experiencing them. Nobody remembers the previous occurrence, to help with salience and first-hand memories of hardships. Therefore, people find it difficult to imagine the consequences for which they may need to prepare. Even in Hurricane Alley in Southern US, where communities get hit frequently, predictably, and memorably, people and institutions are mostly reactive rather than proactively and systematically considering long-term investments in prevention or damage minimization.

Disaster preparedness holds some lessons for combatting localized HW attacks. Japan, where earthquakes occur frequently, has developed ways to build structures resistant to them which greatly diminish losses of life and property. While it is costly to build earthquake-resistant structures, not doing so is far more expensive ex-post. We might adopt this approach for certain types of HW attacks which are quite frequent in both Canada and the US. For example, we might harden vulnerable targets—record systems for hospitals, banks, schools, or government agencies—when we build them, rather than scrambling to respond to attacks.

One enemy of natural disasters and HW responses is lack of redundancy in vital systems. Organizations with data vulnerable to attacks need to safeguard their data in several ways, some completely cut off from external access. While that approach likely adds to the costs of business, it arguably pays off amply in case of attack. And, like Y2K efforts, it runs the risk of being considered superfluous if it works properly!

We can draw some lessons for how to rally communities against HW by examining successes and failures to get people to act against CC threats. CC has been socially amplified much more broadly than Y2K, so there is widespread global awareness. Nevertheless, in the US people consistently dismiss concerns. For example, in 2022 CC

was ranked 14th among 18 top policy worries (Pew Research Center 2022). Like HW, CC belongs in the class of "wicked problems" (Rittel and Webber 1973). "Wickedness" is synonymous with complex and dynamic, defeating attempts to link causes and effects and to learn what works.

Also like HW, CC unfolds relatively slowly over time, dwarfing its threats in people's minds compared to their day-to-day worries. To wit, building along the coasts and even on islands continues apace in Canada and the US, despite predicted[14] sea level rises. We learn that even broad awareness does not necessarily lead to sustained actions. In "The environmental Case," J Layzer (2009) argued that although not sufficient, salience in the public's eye is absolutely necessary for politicians to invest themselves in needed change. HW is not anywhere nearly as socially amplified as CC; what chance does it have to gain the salience necessary for action?

A Massively Parallel Approach

One approach gaining traction in planning is to engage communities in local adaptations that improve living conditions now and may also resist or at least blunt negative CC effects in the long run. These include fixing obsolete electricity, water, and sewer infrastructure, protecting scarce water resources, and drawing up building ordinances that take account of known local risks. These (distributed, locally driven) adaptations might work also against HW infrastructure attacks. They are easier to implement than large-scale policies, benefit residents both now (making investments acceptable) and later, and they match specific local threats. Importantly, they engage community members in their own defense, taking advantage of local knowledge. Although this is a wise and robust strategy, it requires many to engage in advocacy and self-organizing. Burgess & Burgess (2020) called this a "massively parallel" approach when they proposed it for peace building and for addressing social polarization (Burgess et al. 2022).

Large-scale efforts at social amplification of an issue work through coordinated traditional and social media, education institutions, public and private organizations to disseminate information and call to action, as in the case of CC. In contrast, the massively parallel approach relies on numerous localized, short-range interactions among champions of a specific issue and members of a community. Rather than being coordinated and centralized, it tends to be the result of self-organization at the community level, where it promotes actions whose benefit community members, recognize, thereby providing incentives for them to act. The cumulative effect can be considerable. However, this approach requires champions aware of a need, who initiate community interactions to achieve specific results.

The massively parallel approach seems apt for responding to HW because it mimics the characteristics of HW attacks. They too are numerous and distributed and target specific

[14] We also need to recognize that some climate change predictions have already been shown to be off-the-mark (e.g., Pielke et al 2022), which does not help their credibility and undermines efforts to implement sensible adaptive measures.

local vulnerabilities resulting in considerable consequences. Some may be more easily noticed and monitored at the scales at which they occur. A massively parallel response would require both preparedness and response actions stratified across scales, from individuals to local communities, to provinces/states to the national levels. It would need to be adapted to local conditions and decentralized to speed action. It may still be slower than we might wish, as multiparty processes tend to be (Kaufman et al 2018). However, when it gains traction in numerous communities, the massively parallel approach can percolate through entire regions and countries and move politicians and organizations to action. Government entities such as the military defense structures may help sustain such actions through information and technology and, importantly, they may be helped in turn in their own efforts by focusing on the activities only they can perform.

Some Requisites for Responding to HW

We tend to leave to our national governments the task of conducting big defensive/offensive moves against external and internal security threats. I propose that we also need to shoulder part of the responsibility of protecting ourselves through massively parallel actions, instead of relying completely on governments at all levels.

Building public awareness of HW is a necessary first step, just as in the case of climate change. Telling stories in many venues, including social, mainstream and entertainment media about CC consequences around the world has heightened public concern, providing space for public and private organizations to act. Stories are also what moved several of us to participate in Project Seshat. Now think of numerous distributed efforts[15] by defense, policy, law and other professionals and community leaders to disseminate information about HW, to bring it in the open and to change its status from conspiracy theory to the serious threat that it is.

Massively parallel actions to counter HW can operate at different scales, from local to national. A few suggestions follow.

At the individual and community (eye) levels, some relatively low-resource steps are possible, including:

- Persuading individuals about the reality of HW and need to prevent it, and offering advice for personal and for organizational data protection;
- Encouraging self-reliance and strengthening local communities' vigilance;
- Taking simple steps to harden critical local targets and make it difficult/costly to access/damage data;
- Devising protocols for recovery, including decentralized backups for essential data;
- Developing alert systems for suspicious local activities, such as outsiders buying agricultural land or other local resources, especially near defence installations;

[15] Arguably, China has been working in massively parallel mode around the world for a while, positioning assets and gathering information internationally; we could emulate it, matching complexity with complexity.

- Increasing and maintaining public awareness through various channels by enlisting local media, schools, entertainment, social media and technology means.

At higher organizational/government levels (province/state) defensive actions could entail:

- Dedicating public and private resources for developing and routinizing vulnerability scanning practices, to identify how HW could hit critical systems singly and in percolation fashion - whereby an entire system is suddenly disabled as a result of numerous small, difficult to detect moves over time;
- Creating *wicked* scenarios for HW-disrupted critical systems such as food, energy, water/sewer, communications, and supply chains at different scales, not all derived from past incidents, since HW attacks are increasing in variety and sophistication, and channels; then engaging in simulations to generate prevention and defense moves, including clear lines of responsibility (who does what, when); and conducting pre-mortems (Kahneman et al 2011) on scenarios to uncover vulnerabilities and remedy them;
- Decentralizing (and in some cases disconnecting from each other) communication, banking, energy production, and other vital networks, and building redundancies in them to limit HW damage by preventing disruptions from cascading throughout the networks like epidemics;
- Creating *plans B* for restoring critical systems (water, electricity, and communication networks) once they are disabled by HW actions; scenarios can be helpful here too, for imagining what would happen if vital systems failed or did not exist, and identifying actions that restore functionality;

The highest (national) government levels have responsibilities and resources for:

- Conducting preemptive HW and other kinds of retaliatory attacks, whether diplomatic, economic or even kinetic, to deter;
- Reducing the predictability of their responses;
- Allocating resources and providing technical assistance to help organizations and communities protect themselves against HW attacks;
- Supporting broad dissemination of information about HW and lending it credibility;
- Shoring up protection of national vulnerable sites and equipment;

Finally, international cooperation among governments of free nations is also necessary. Although we don't always recognize our similarities, Canada and the USA share not only a continent but also culture, similar economic systems, parallel layers of government—from national/federal to provinces/states to local—and joint interests, one of which is preserving their respective democracies and individual freedoms. HW attacks against one are bound to spill over hurt the other too. For example, when airplanes were grounded everywhere in the US for a day

in January 2023, the same happened the following day in Canada although no sign of a nefarious attack (or any other reason) has been disclosed yet to account for these unique events.

However, there is one difference that might be meaningful to how HW operates: Canada's population represents a relatively small fraction of the USA population (roughly 10%). Its economy is correspondingly smaller, as is its defense capability. Does this matter to the ability to respond effectively to HW attacks? It is likely that it does. Therefore, efforts to defend against HW can only benefit from cooperation at all levels, mutual learning and assistance. To help each other and themselves effectively against HW, the Canadian and US governments may engage in

- Sharing information with each other and with other HW-target countries to speed up learning how to recognize and prevent HW attacks;.
- Sharing intelligence about those who sponsor, fund and execute HW attacks;
- Coordinating strategies of defense and supporting each other in international fora and in preemptive use of HW against opponents.
- Sharing technologies which prove beneficial in preventing or recovering from HW attacks on vital systems.

Do negotiations have a place among anti-HW strategies? To begin with, we need to sharpen our ability to recognize when negotiation is not a possible response, and we need to move to a different mode of thinking than traditional diplomacy. However, we can still negotiate with high-level sponsors of HW, communicate consequences, and implement them when necessary.

While we can hardly hope to engage effectively with covert opponents, negotiation is a key modality for rallying our own side. As well, within a country, at every scale, we make joint decisions to defeat HW through negotiations. Devising and implementing various defense and preparedness initiatives involves engaging with numerous stakeholders, diverse in interests, values, and knowledge, to negotiate broadly acceptable measures. These may require investments of scarce resources, and sometimes accepting limits on certain preferred activities or how we engage in them, to increase safety. Massively parallel joint efforts to disseminate information and act on it may become central to efforts to redirect some resources away from publicly favored objectives to defending against HW threats.

Project Seshat , with its interdisciplinarity and increasing reach, illustrates how massively parallel initiatives to counter HW get started, but many more efforts by many are necessary to rise to the “massive” level.

References

Axelrod, Robert. "Effective choice in the prisoner's dilemma." *Journal of conflict resolution* 24, no. 1 (1980): 3-25.

Bialek, Janusz. "What does the power outage on 9 August 2019 tell us about GB power system." *Cambridge Working Papers in Economics* (2020).

Biello, David. "Is the US grid better prepared to prevent a repeat of the 2003 blackout." *Scientific American* (2013).

Burgess, G., and H. Burgess. "Massively parallel peacebuilding." (2020). https://www.beyondintractability.org/frontiers/mpp-paper (last accessed on 12.3.2022).

Burgess, Guy, Heidi Burgess, and Sanda Kaufman. "Applying conflict resolution insights to the hyper-polarized, society-wide conflicts threatening liberal democracies." *Conflict Resolution Quarterly* 39, no. 4 (2022): 355-369—feature article.

De Cock, Christian. "Of strategy, warfare and fiction: writings on Sun Tzu." *Asia Pacific Business Review* 4, no. 2-3 (1998): 157-161.

Duggan, Maeve, Amanda Lenhart, Cliff Lampe, and Nicole B. Ellison. "Concerns about children, social media and technology use." (2015). https://www.pewresearch.org/internet/2015/07/16/concerns-about-children-social-media-and-technology-use/ *(last accessed on 12.3.2022).*

Kahneman, Daniel, Dan Lovallo, and Olivier Sibony. "Before you make that big decision." *Harvard Business Review* 89, no. 6 (2011): 50-60.

Kaufman, Miron, Sanda Kaufman, and Hung T. Diep. "Statistical Mechanics of Political Polarization." *Entropy* 24, no. 9 (2022): 1262. https://doi.org/10.3390/e24091262; special issue: Statistical Physics of Opinion Formation and Social Phenomena—feature article.

Kaufman, Sanda, Connie Ozawa, and Deborah Shmueli. "Negotiations in the public sector: Applying negotiation theory to multiparty conflicts." *Négociations* 29, no. 1 (2018): 59-73. Special issue, *Négociations* 29/1: 59-73.

Kile, James C., Stephen Skowronski, Mark D. Miller, Stephan G. Reissman, Victor Balaban, Richard W. Klomp, Dori B. Reissman, Hugh M. Mainzer, and Andrew L. Dannenberg. "Impact of 2003 power outages on public health and emergency response." *Prehospital and Disaster Medicine* 20, no. 2 (2005): 93-97.

Ko, Jae-Young "An Explanation of the 2021 Jackson Water Crisis and Policy Suggestions for Sustainable Water Infrastructure in Jackson, Mississippi---A Research Commentary." *Challenges of an Aging Water System: The Jackson Water Crisis---A Research Commentary*, 56.

Layzer, Judith A. *The environmental case: Translating values into policy*. CQ Press, 2009.

MacGregor, Donald G. 10 Public response to Y2K: social amplification and risk adaptation: or, how I learned to stop worrying and love Y2k. *The social amplification of risk* (2003): 243-261

Pielke Jr, Roger, Matthew G. Burgess, and Justin Ritchie. "Plausible 2005-2050 emissions scenarios project between 2 and 3 degrees C of warming by 2100." *Environmental Research Letters* (2022).

Reilly, Peter. "Was Machiavelli right—lying in negotiation and the art of defensive self-help." *Ohio St. J. on Disp. Resol.* 24 (2008): 481.

Rittell, H. W. J., and M. M. Webber. 1973. Dilemmas in a general theory of planning. *Policy Sciences* 4: 155-169.

Shmueli, Deborah F., Connie P. Ozawa, and Sanda Kaufman. "Collaborative planning principles for disaster preparedness." *International Journal of Disaster Risk Reduction* 52 (2021): 101981. https://doi.org/10.1016/j.ijdrr.2020.101981

Taleb, Nassim Nicholas. *The black swan: The impact of the highly improbable*. Vol. 2. Random House, 2007.

Tyagi, Anubhav. "TikTok Might Soon Get Banned In The US." Techworm, June 29 2022. https://www.techworm.net/2022/06/tiktok-might-soon-get-banned-in-the-us.html (last accessed on 12.3.2022).

Vogels, Emily A., Risa Gelles-Watnick, and Navid Massarat. "Teens, social media and technology 2022." (2022). *Pew Research Center.* https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/ *(last accessed on 12.3.2022).*

"Public's Top Priority for 2022: Strengthening the Nation's Economy." (2022). Pew Research Center. https://www.pewresearch.org/politics/2022/02/16/publics-top-priority-for-2022-strengthening-the-nations-economy/ (last accessed on 12.3.2022).