Midnight in a Kaleidoscope: Conflict Management and Hybrid Warfare

Adrian Borbély & Chris Honeyman

Why a book of scenarios about hybrid warfare designed for non-military people?

Fair question! The short answer is that one characteristic of hybrid warfare, which will become apparent in the scenarios which follow, is that it affects us all: everyone should feel concerned. A central condition of below-the-surface foreign aggressions is that they are not limited to a classical battlefield, i.e., a localized region where armed forces shoot at each other trying to take each other's positions. In hybrid warfare, society as a whole is the battlefield.

Below, we will discuss in broad terms the current state of relevant teaching in several key fields and articulate our conception of what is now needed to address hybrid warfare. But first, it is essential to note the rising public perception of hybrid warfare; to discuss at least briefly how our societies got to this point; and to assess what is currently being done about it. In all these areas, for reasons which follow, our focus will be on those parts of Western societies and economies which do not have the resources of national governments.

Public perceptions of hybrid warfare (ca. early 2025)

"Grey zone conflict" and "hybrid warfare"[1] are just two among several terms currently used to depict the same thing – assaults against a nation, its citizens and its private enter-

[1] Confusion over these and other terms is common; see Leonard Lira's and Bryan Reyes' chapter for an explanation of how such overlapping terms developed. We endorse their recommendation that in future, those discussing this whole topic area could clear the decks by adopting a newer catchall term, "hybrid conflict." However, fifty Project Seshat contributors, in numerous discussions over several years, settled on "hybrid warfare" as a working expedient, and we decline to suddenly disturb that. We are accordingly using "hybrid warfare" for the time being, throughout this book.

prises, as well as public and NGO actors.[2] These attacks may or may not involve a military component and may be executed by entities seemingly unconnected to another country's national security forces. Even after an attack, its true intent may remain quite obscure. For example, the well-known Colonial Pipeline attack of 2021, which resulted in widespread economic damage after a pipeline carrying 45% of the U.S. East Coast's oil supply was shut down for nearly a week, was claimed by the attacker to be a purely money-oriented attack with no broader consequences intended.[3] Reportedly the attack was facilitated by such poor security practices at the pipeline company that the theft of a single password was all that was needed, suggesting in turn that such a major attack could conceivably have been mounted by a relatively "amateur" group.[4] Yet the group involved is widely believed to be based in Russia, where government support of such private crime groups is widely known,[5] and denial of all sorts of government-supported hybrid attacks has become routine.

A scant five years ago as of writing this, "hybrid warfare" was still an obscure enough concept that when contacted by Honeyman during the fall of 2019, hardly any among dozens of conflict management veterans admitted to having even heard the term before. But now it is increasingly recognized as a matter of public concern; for example, a November 2023 daylong public event on the subject, mounted by London's Imperial War Museum, sold out.[6] The UK Ministry of Defence's pithy quote on the flyer for that event read: "The international consensus on hybrid warfare is clear; no one understands it, but everyone agrees it is a problem."

This book's particular intent is to shed light on attacks targeting entities beyond national governments, for several reasons. First, campaigns of hybrid warfare coordinate activities among private, government and nonprofit entities. They routinely use tools aimed at nonmilitary targets, including cyber tools, public or commercial corruption, transnational organized crime, disinformation campaigns, and various other methods.[7] And deception, including denial that any such attack is underway, is a standard element

[2] Hybrid warfare is still a new enough topic that many audiences require a basic explanation. This discussion has been adapted for the present book from prior related publications designed for other audiences; see e.g. Chris Honeyman and Rachel Tan Xi'En, 'A New Management System, for a New Type of Conflict? Singapore's Possible Role in Managing Grey Zone Conflict in International Commerce' (Dispute Resolution Review (Australia) Vol. 4/2: 99-119 and directed to a public policy audience); Chris Honeyman and Andrea Kupfer Schneider, 'Hybrid Warfare: Fighting Back with Whole-of-Society Tactics.' (2023) 30 On Track 6 (for a Canadian military audience); Chris Honeyman and Andrea Kupfer Schneider, 'Introduction: Negotiation Strategies for War by Other Means' (2023) 24 Cardozo Journal of Conflict Resolution 487 (in an American legal and dispute resolution context.) It also draws extensively on previous writings by several security colleagues quoted below, particularly Christopher Corpora, Leonard Lira and Steven Desjardins.

[3] Freed, A.A. blog: Inside the DarkSide Ransomware Attack on Colonial Pipeline. https://www.cybereason.com/blog/inside-the-darkside-ransomware-attack-on-colonial-pipeline

[4] "One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators." https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/

[5] See e.g. Galeotti, M. 2018. *The Vory: Russia's super mafia*. New Haven: Yale.

[6] From Sniper to Smartphone: Hybrid Warfare and the New Face of Conflict' Imperial War Museum (Web Page): www.iwm.org.uk/events/from-sniper-to-smartphone.

[7] Galeotti, M. 2023. *The Weaponization of Everything: A Field Guide to the New Way of War*. New Haven: Yale.

in creating an atmosphere of ambiguity, and in parallel, the attacker's desired state of mind among defenders: doubt and confusion.[8] Additionally, it is evident that Western intelligence, military and other security agencies are not (yet) effectively organized to respond strategically or coherently to such actions impacting non-military sectors.[9]

Hybrid warfare in history

It is important to emphasize that what we are seeing today as hybrid warfare is new in its variety, as well as the sheer volume of activity, and of course in many of the specific techniques used – but not in its essence. In a previous Project Seshat publication,[10] Christopher Corpora noted that present-day hybrid warfare has many precedents:

> … Hybrid Warfare and Gray Zone Conflict are recent terms used to understand and explain an age-old human social phenomenon – attaining dominance and influence without throwing a punch or firing a shot. Versions of this strategic concept have existed throughout history, but they have been evolving more rapidly in the modern era. Asymmetric Warfare, Military Operations Other Than War (MOOTWA), Irregular Warfare and Active Measures are a few of the terms used over the past 50 years to describe non-conventional strategies and tactics for weakening an enemy, ideally limiting the amount of conventional force needed to win. Softening an enemy through psychological or physical deception led to many great classical victories in war – ranging from Egyptian fighters in baskets, through Alexander's famous deception in the conquest of Punjab, to the Trojan Horse. The price of war increasingly became a point of focus, as the costs rose, in terms of both blood and treasure, forcing policymakers to think carefully about direct combat as a viable option to gain power and pursue their interests. Hybrid Warfare and Gray Zone Conflict are updated versions of this indirect aggression – using unconventional means and targeting a broader community outside the traditional combatant space and enabled largely through the internet (or cyberspace as some call it). The creation and growth of the internet over the past 40 years provided a new domain for contestation, joining air, land, sea and space as places for international competition. It also is a space of easy intersection with the private sector,

[8] Christopher A. Corpora, How to Undermine a Nation-State in 120 Days: Mediation and Negotiation in a Hybrid Warfare World (2023) 24 Cardozo Journal of Conflict Resolution 503. See also Steven Desjardins, Hybrid Warfare – Is it New, is it Real, and What are the Threats, Vulnerabilities, and Implications for Defence and the Military? 30 On Track, Winter 2023

[9] Scott Tait, Hybrid Warfare: the New Face of Global Competition, Financial Times: https://www.ft.com/content/ffe7771e-e5bb-11e9-9743-db5a370481bc.

[10] Corpora, above at fn 8. (Internal citations omitted.)

which is the domain where most Hybrid War actions occur – ranging from indirect manipulation through disinformation operations to cyber blackmail and denial operations. The locus of these Hybrid War activities purposefully targets "civilian" and "commercial" interests to instigate chaos and create unignorable disruptions, where scarce public resources must be expended to respond, and private legal actions are required to address the impact… Hybrid warfare, as the latest term or euphemism for actions other than the use of conventional violence to advance national interests, has grown rapidly in importance since the end of the Cold War, coinciding with the advance of cyber and communications technologies. State and non-state actors now use the tactics associated with hybrid warfare to:

- Undermine an adversary's ability to pursue its own interests and/or thwart the attackers.
- Reduce public and market confidence in the adversary at all necessary levels – global, regional and local.
- Instigate confusion, chaos and internal conflict to deflect an adversary's attention, resources and self-confidence.
- Promote state and organizational interests in opposition to the adversary's potential gains.

Historically, the kinds of deception and sabotage described above resulted in eventual fighting. This strategy has always involved the strategic positioning to develop and leverage non-conventional means or tactics to weaken an opponent, preferably with little to no attribution – allowing for success by default, with tumult inside an adversary's camp. Sun Tzu makes one of the earliest mentions of this strategy, saying, "To subdue the enemy without fighting is the acme of all skill," and, "The supreme art of war is to subdue the enemy without fighting." Another long-respected military theorist, Carl von Clausewitz, said, "[t]he best form of defense is attack" and, "[a]ll war presupposes human weakness and seeks to exploit it." Although his own intentions were literal, the broader application of this idea provided a theoretical space to spark more purposeful thinking about taking offensive actions in advance of direct conflict, either to soften the adversary or to sufficiently deter it from contesting an issue. Clausewitz also recognized the relationship between politics and war, calling the latter an extension of the former. Hybrid Warfare occupies a space be-

> tween conventional politics and war, which is why many of the tactics are shared across the domains. Deception, disinformation and sabotage are all important competencies for the modern political operator. The increased capability and public reliance on the internet have increased the span and effect of such techniques. The outcomes are seen daily across various media and polemic websites.

Similarly, Steven Desjardins[11] points out that:

> … 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… 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, 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.

Outlining a series of technological developments, Desjardins goes on to state that:

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

And in a detailed review of the military and security literature related to hybrid warfare,[12] Leonard Lira and Bryan Reyes note that:

[11] Desjardins, above at fn 8. (Internal citations omitted.)

[12] We took this quote from the unpublished paper that was used as a basis for drafting two chapters of this book, the Lira and Reyes terminology chapter, as well as the selected readings bibliography presented at the end of this volume.

> … Initially, hybrid threats were only seen as asymmetric strategies employed by non-state actors such as terrorist groups residing in countries like Lebanon, Syria, Pakistan, Afghanistan, or Iraq. Scholars observed that these groups would blend conventional and irregular capabilities specifically targeted at US vulnerabilities to draw out conflict in hopes to achieve their goals. However, the invasion of Ukraine by Russia, and earlier examples of Russian hybrid attacks employed against Estonia, and Georgia, demonstrated a shift from only non-state actors employing hybrid threats to state actors colluding with non-state actors to employ these techniques in conflict. The shift of state actors purposefully engaging in grey zone conflicts demonstrates the dilemma of how to respond to low aggression conflicts that fall below traditional threshold descriptions of warfare. Aggressors employing hybrid threats in the grey zone could operate within the wording of international treaties and laws like UN Security Council's Article 51 guarantee of self-defense and NATO's Article 5 mutual defense treaty and not trigger a united international response. Other challenges to international laws, such as China's build-up of artificial islands to extend their claims to the South China Sea, diminished the integrity of international laws. These examples exposed 'weaknesses' in international security regimes and allowed adversaries to exploit blurred lines of sovereignty, rules, and laws, to gain an advantage.

Current responses to hybrid warfare, effective and otherwise

Responses from the targeted entities are often unhelpful and ineffectual, ranging from denying the occurrence of any attack to threats of retaliation, or proposing increasing defense expenditures at the government level or severing all dealings with countries responsible for these attacks.[13] Although each of these reactions may have its place, none of these responses has proven generally effective. Thus, it is imperative to develop a comprehensive approach so that hybrid warfare can be better comprehended as a category and managed on an overarching level – as distinct from countermeasures that are overtly retaliatory on a military scale.

At the same time, as Corpora and Desjardins note above, the direct roles and vulnerability of all kinds of non-governmental entities have vastly increased. For one thing, in a globalized economy, "business and NGO executives, and critically, their 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

[13] See articles cited in note 2.

transactions to have hybrid warfare connotations."[14] For instance, if a seemingly "domestic" company with which a city government is contracting for water or other utilities, transportation, communication networks, or a myriad of other services, is covertly influenced by a foreign government, the city might become a target without recognizing the opponent's intention or even its existence.[15] Dealings with innocent third parties can have the same effect in the private sector. A conspicuous example was the NotPetya virus, which was used by Russia in a cyberattack on Ukraine in 2017 – and which was so overeffective that it spread to thousands of companies that were not targets at all. In the most startling result, the infection of a single computer at a Ukrainian branch office of Maersk, the world's largest shipping firm, spread throughout the firm's internal networks, and resulted in the entire company effectively shutting down for an extended period.[16]

Meanwhile there is compelling evidence not only that the private and nonprofit sectors are significant target areas in hybrid warfare,[17] but that they are even less prepared for this than governments. What's more, many of these attacks 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.

Efforts to respond to hybrid warfare at the strategic level are ongoing, with recent events, particularly the Russian invasion of Ukraine, elevating their prominence. However, the critically important tactical and operational responses often occur in widely dispersed corporate boardrooms, law offices, municipal government or university offices, etc. Many who are unwittingly involved in a hybrid warfare attack have little or no understanding of the phenomenon, and even those who are aware of an attack are often poorly informed about what actions they can take.[18]

As Corpora and Desjardins point out, efforts to undermine a perceived rival nation without triggering open warfare are not new; such practices date back thousands of

[14] Chris Honeyman and Andrea Kupfer Schneider, 'Introduction: Negotiation Strategies for War by Other Means' (2023) 24 Cardozo Journal of Conflict Resolution 487.

[15] See the discussion of the SolarWinds attack in Leslie, A. 2023. 'Redefining Contours of "Business as Usual" and the Potential Role of the Military.' In Hybrid Warfare: Fighting Back with Whole-of-Society Tactics, 30 On Track 28, Winter 2023.

[16] Daniel E. Capano, 'Throwback Attack: How NotPetya accidentally took down global shipping giant Maersk', Industrial Cybersecurity Pulse (online at 30 September 2021): https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/

[17] Case after case the evidence has accumulated in recent years. For those still inclined to treat the stories as anecdotal, we can recommend Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: People's Liberation Army Publishing House, 1999). There is no more authoritative source than these two Chinese army colonels, who originally set forth what has since transparently become China's strategy for hybrid warfare against the West. A selection of short phrases from Qiao and Wang (as used throughout the book by an artist who created a series of weavings to illustrate hybrid warfare) will give the general idea: "erode economic strength", "this war is not a war", "a borderless battlefield", "this information is not information", "undermine the legitimacy of key institutions", "remember your future", "paralyze decision making", "encourage social discord", "delay recognition an attack is underway", and last but not least, "Some morning you may awake to find that the gentle and kind things around you have begun to have lethal and offensive characteristics." See also 'Gentle and Kind Things', Rachel Parish (Blog Post), https://rachelparish.com/projects/gentle-and-kind-things/

[18] Calvin Chrustie, 'Mind the Hybrid Warfare Gap' (2023) 30 On Track 12

years. Yet there is something new here. Sanda Kaufman distinguishes the new style of attack from long-used methods of undermining opponents in these terms:

> … Perhaps a key difference between hybrid warfare and historic deceptive methods of prevailing over enemies is the use of sophisticated technologies applied to ever more complex situations. Hybrid warfare 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.[19]

Current related teaching in business, law and other professional schools

We believe not only that the topic of hybrid warfare matters to us all, but that it is currently in an educational blind spot, stuck in an intermediate zone between macro/systemic risks on the one hand, and micro risks on the other hand.

When it comes to macro risks, European business and law students are routinely taught about geopolitics, while their American counterparts are in general much more focused on affairs within their home country. Across these domains, such teachings remain mostly disconnected from their future fields of action: throughout the West, geopolitics is taught as an element of context, rarely as something that could intrude into everyday operations. As such, in business schools, geopolitics is taught because it is useful for making sound decisions on financial markets, to help tailor the right international supply chain, or to decide whether to enter a new market. However, students – and professionals alike – are not told that geopolitics may directly impact them, or their organization, as a target or as an accessory to morally-disputable activities.

Regarding micro risks, business and law students are taught that compliance is a requirement to avoid legal troubles, as well as business and reputation costs. Most of them are also made aware of everyday risks such as occupational illnesses, cashflow issues and contractual incidents (e.g., late deliveries' impact on a supply chain) – and how to respond to them.

What sits in between such "regular" risks (micro) and exceptional risks (macro) may, in general, be in a blind spot for future business leaders, managers and lawyers. It is in such an intermediate layer that hybrid warfare hides.

[19] Sanda Kaufman, How Should the Whole-of-Society Respond to Hybrid Warfare? (2023) 30 On Track 47

Meanwhile, future diplomats and military officers are taught that countries compete with one another using four distinct instruments (acronym DIME). A thumbnail sketch might look something like this:

- Diplomacy: traditionally, diplomats interact with governments and among them; they pass messages to each other and report home about foreign government policies, society's impulses and economic development trends. Diplomats are also used to building coalitions and confidentially expressing warnings and threats.
- Information: each country builds its own narrative and communicates it on the international scene through its culture and the internationalization of their economic champions. The line between this and propaganda is difficult to ascertain. On a different level, diplomats also gather information about the state of the world and the actions of various foreign governments. Information also includes intelligence and, hence, spying activities.
- The military serves both as a dissuasion mechanism and a way to advance a state's interests. Today, it is used as the last option, when everything else has failed. Countries invest heavily in their armed forces. In addition to their classical roles, military forces are also used to preserve peace, for emergency crisis response and for humanitarian purposes (also by third parties to tip the balance in favor of the friendlier party in open conflicts).
- Economic: countries cooperate and compete economically, within the rules of the World Trade Organization and various bilateral and regional economic exchange treaties. They may use private companies and/or public sector entities. Countries measure their influence on the international scene based on their GDP and their trade surplus or deficit. Sovereign debt is also exchanged, with or without strings attached.

Traditionally, each of these instruments has its own rules, the most well-known being the rules of war established through various treaties and international conventions. Players are accustomed to the rules of their own field of action, while the other fields may be totally foreign to them. In a European business school, students will learn about Economic, maybe a bit about Information (through academic exchange programs) and Diplomatic (through geopolitics courses). Law students may not hear much about any of the four instruments.

Hybrid warfare, turbocharged by globalization and information technology, is blurring lines and has created a less-regulated environment where new forms of influence and power are at play. One common factor is that these do not have to comply with the

rules of war and as such may have a broader base of possible targets. In effect, warfare, previously limited for practical purposes to military and political circles, may now spill over to all of society.

In this new environment, public planning, business and law students – and citizens in general – should be taught that geopolitical games may infiltrate their everyday lives. But so far, they rarely are. Hence the idea behind this book.

Examples of warfare pervading society are numerous:

- Lawyers may register companies that are fronts for foreign State-supported activities (including criminal networks), and then work diligently to keep them "below the radar" by staying, as far as possible, in apparent compliance with local laws.
- Entrepreneurs looking to finance their start-up through global finance and venture capital may be unaware that foreign States may use such financial mechanisms to hijack patented technology, or to preserve their own, national companies.
- Public services may be the target of disinformation campaigns or cyberattacks by foreign States looking to cause chaos within a competing country's population.
- In court, lawyers may be defending people who are in fact foreign assets, or be representing, consciously or unconsciously, foreign agents using "lawfare" to advance foreign interests (e.g., to silence opponents among its diaspora).
- No matter who you work for, cyber incidents may be triggered by State-sponsored cybercriminals looking to access sensitive data – or trying to force you to pay a ransom to finance their other unlawful activities, or even their armed forces.
- Data theft may, on the one hand, be a purely criminal endeavor (aiming to capture a ransom payment). On the other hand, once harvested, such data may be copied over to a foreign nation's intelligence services and reused to sway public opinion, or to target individuals to use to their own advantage, sometimes as "useful idiots."
- On social media, people may be induced to push opinions that are in fact propaganda tailored by a delinquent foreign nation.

- Elections, supposed to be free and fair, may be subjected to external forces (disinformation, illegal financing and/or corruption) to pursue goals such as destabilization or the installation of "friendly" leadership.[20]
- Participation in a demonstration or resistance movement may in fact have been incited by a foreign nation looking to gridlock an adversary.
- Law enforcement personnel may try to dismantle transnational criminal activities (such as drug trafficking, or money laundering) without awareness of the links between these criminals and foreign states.
- University researchers may be collaborating with scientists who are secretly funneling data and knowledge to a foreign nation's army labs.[21]
- Journalists who are close to uncovering hybrid warfare mechanisms at play (or even their family members) may be threatened, or sued, to silence them or to deter other journalists from investigating.

And this list is far from exhaustive.

In other words, the world is not only more dangerous than what initially meets the eye, but the dangers directly affect a far broader swath of the population than has previously been the case.

When one of these mechanisms comes into someone's view, there is still a strong tendency to approach the risk as isolated, instead of taking a systemic approach that would include all hybrid warfare at play simultaneously. The same myopia applies to the links between kinetic actions (armed forces in action) and hybrid warfare mechanisms (e.g., cyberattacks). Taken by itself, for instance, any one such action might seem, if not innocuous, at least limited in its possible harms. "Yes, a Russian cybercriminal group attacked our company. So what? We've paid the ransom / fixed our servers / restored our data / improved our internet security, and this has happened before to lots of companies." However, if the attacking group is backed by Russian military intelligence; if it has also attacked other companies in a domain that may have strategic significance; and if, in parallel, other actions, such as disinformation campaigns, are launched on our country – well, taken together, these events paint a completely different picture, do they not? Students in many fields now need to be trained to evaluate that picture, and to respond effectively as part of their future employment – but to begin with, they must be trained even to perceive that picture.

[20] Recent examples include Georgia (https://www.politico.eu/article/georgia-elections-marred-by-intimidation-and-interference-observers-warn/) and Romania (https://www.ifes.org/publications/romanian-2024-election-annulment-addressing-emerging-threats-electoral-integrity).

[21] See e.g. https://www.striderintel.com/newsroom/strider-technologies-launches-new-tailored-platform-to-safeguard-academic-research-from-emerging-global-threats/

All these reflections should lead us to an unsettling conclusion: the line between war and peace is now blurred. We may be officially at peace with nations that use hybrid warfare to destabilize us, working hard to stay beneath the level of conspicuousness that would trigger a reaction from us. This should in turn lead to some difficult conversations: are we truly at peace with Iran? With China? Are Iran, Russia, or North Korea just messing with their immediate neighbors, or engaged in what amounts to a global war against the western world? In the answers to these questions lie strategic challenges that need to be addressed.

Add to this that what constitutes hybrid warfare may be subject to definition issues. Beyond the definitions and descriptions above, and broadly speaking, some common indications of a hybrid warfare incident include:

- Some illegal activity is taking place, or a democratic instrument is hijacked to serve the interests of some to the detriment of others.
- The incident benefits the interests of a foreign nation.
- That foreign nation may be pulling the strings, despite its public denial.
- The incident takes place in a context of distrust, exacerbated competition and/or latent or open conflict between the country of the target and the suspected attacking nation.

The fact that several such mechanisms are at play concurrently is a particularly strong indicator that we may be in a hybrid warfare situation.

Hybrid warfare is also a moving target. It relies on public policy weaknesses (permissive laws) and on information technologies. It thrives in the freedom space that our Western democracies represent. And its elements evolve fast. Progress made in one area may even inadvertently open another door for new destabilization mechanisms. We are writing these lines in January 2025: we can confidently expect some new avenues for hybrid warfare actions to appear shortly, even as some existing ones may be effectively closed.

The role of expertise in conflict management and negotiation

Some will undoubtedly ask:[22] *What do negotiation and conflict management have to do with any of this?*

To anyone who has been following the news these past years, it should be self-evident that the expertise and diligence of military and security forces, even with their vast budgets, have not been enough to forestall a rapid rise in attacks on Western populations via their economic, social and political infrastructures. But there are many lenses through

[22] It is worth noting that most of the conflict management experts Honeyman initially approached asked exactly this question, and/or its corollary "What does any of this have to do with my work?" The answers apparently convinced them, because the vast majority of those canvassed subsequently joined Project Seshat.

which conflict has been studied, and multiple disciplines in which knowledge and skills have led to the development of different tools for working on, with or through conflict.[23]

By 2019, there was at least one security expert (Calvin Chrustie) who had enough experience of how other kinds of conflict management experts worked to see how working with them might help. Project Seshat was formed specifically to create such a working collaboration, starting with an arena for security experts and legal, negotiation and other conflict management scholars to meet and discuss possibilities. During the fall of 2019, Honeyman recruited about 40 conflict management experts from a wide range of fields for the new project; Chrustie meanwhile worked to recruit a dozen security experts willing to engage with these unfamiliar species of professionals, and though some of them required more convincing than others, he eventually succeeded.

These two worlds have rarely interacted in the past, and people with expertise on both sides are rare indeed, so we would like to commend all our colleagues in that effort for their openness to working in an unfamiliar way. We would also like to express our gratitude for their level of real commitment: their efforts over years have not only been for zero pay, but at their own expense for several related costs, such as travel to meetings. If any further difficulty were needed, the project formally launched just weeks before the covid pandemic struck. Once drawn into the discussion, however, the group was not easily daunted, and by the fall of 2020, following copious and trenchant advice from many project members, the project steering committee was able to publish an article laying out the strategy the group had developed to make some progress in the face of these hurdles.[24]

This centered on using remote meeting technology to form and support five teams, each of which was chartered to write one realistic hybrid warfare scenario. Each team included a cross-section of conflict management expertise from multiple fields, along with at least two security experts (with quite different backgrounds from each other.) It speaks for itself as to the effectiveness of this approach that the teams ultimately produced not five, but eight scenarios, which became the foundation for this book. Borbély has since recruited authors for four additional scenarios which round out the topic areas addressed in this work.

We believe the result is the most comprehensive and realistic scenario-based approach now available for the study of hybrid warfare, and for improving the potential for using knowledge and skills far removed from military and security training to help deal with it. Indeed, among many recent books on hybrid warfare there are very few actual teaching texts of any kind.

[23] For example, Honeyman is also co-editor of *The Negotiator's Desk Reference* (DRI Press 2017), the most comprehensive work yet attempted in the search for an overall understanding of human conflict and what can be done about it. The salient point here is that this two-volume reference not only required over a hundred expert contributors to write it but that they came from some 40 different scholarly disciplines and practice specialties.

[24] Honeyman, C., Chrustie, C., Schneider, A.K., Fraser, V. and Jordaan, B. 2020. Hybrid Warfare, International Negotiation, and an Experiment in 'Remote Convening'. Negotiation Journal, Fall 2020. This article also discussed some further details of the case design strategy which we are not repeating here.

And yet, hybrid warfare demands that we continuously revisit, challenge, and improve our theories regarding negotiation and conflict management. For those – and they are many – who believe "negotiation" and "conflict management" apply primarily to the relationship between the principal parties and/or their named agents, such as attorneys, we offer some simple, yet (we hope) thought-provoking questions:

- Since the puppet master stays hidden and denies any involvement, and since the attacker himself may be an underling or subcontractor who may not be told the big picture behind his actions, whom could we negotiate with?
- Since the attacker's bosses' true objective may be to sow chaos through the attack, while it is the underling who seeks to get money or some form of promotion, when the attack has taken place, what is left to negotiate? In other words, when a maniac takes hostages, we can offer to trade for the hostages with what the offender truly wants – money, freedom… But if those really behind the attack have reached their objective as soon as the attack is effectuated, there may be nothing useful to us left to trade for.
- We may be dealing with bad-faith actors who will never reveal their true interests and objectives. How do we integrate "unspeakable interests" in negotiation?
- Would our collaborative negotiation and conflict management methods work between "the parties" in *any* hybrid warfare scenario?

Clearly theories around interests, or Best Alternatives to a Negotiated Agreement (BATNA), need revision to prove useful in hybrid warfare scenarios.

Yet even with this new set of challenges, in other ways, negotiation and conflict management skills may be key if we want to create resilient societies and organizations. When a crisis hits, people need to interact (sometimes for the first time) both to coordinate and to prioritize. These processes require the skills of a thoughtful negotiator. The "behind the table" parties to these negotiations need to discipline themselves to postpone assigning blame until the impact of the crisis has been evaluated, controlled and erased. They need to communicate with other key stakeholders (lawyers, insurance companies, clients, suppliers, staff…). And these "behind the table" negotiations will likely be essential even where negotiation between the principal parties is impossible.[25]

Even before a crisis strikes, organizations which take to heart these concerns and redesign themselves for the necessary collaborations will be better equipped. Such resilience may indeed be the best anticipation mechanism. And in this area, the already-

[25] Art Hinshaw, Adrian Borbély and Calvin Chrustie, Where is Negotiation in Hybrid Warfare? 24 Cardozo Journal of Conflict Resolution 517.

worked-out teachings about the importance of preparation, as well as many other aspects of negotiation, stand ready for adaptation.

To be more specific, we believe that guarding against attacks, even more than formulating effective responses to an attack, is where the field of conflict management / negotiation really has the most to offer. Yet again, it must be emphasized that this requires a shift in thinking: the "negotiation" most directly relevant here is simply not the kind most people think of first, i.e. what happens directly at a bargaining table with "the parties." In hybrid warfare, for all the reasons noted above, direct negotiation between the attacker and the target is currently unlikely, with limited exceptions such as in ransomware attacks.[26] 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.

Several articles cited here[27] and in the following footnotes show how conflict management scholars affiliated with Project Seshat have already begun to review existing conflict management literature and findings and to distinguish the parts that seem most useful in the hybrid warfare context. In this new environment, pursuing the path thus opened will involve consultation and cooperation among different professional communities on who assumes what roles and responsibilities as part of a broader conflict management strategy.[28]

We cannot emphasize too strongly that the "behind the table" negotiations – in other words, the negotiations between many players who are nominally on your own side – are where "the action" really is. These often-obscure negotiations are incredibly important in averting, preparing for, or responding to a hybrid warfare attack.[29] A hybrid warfare attack on a company that has not prepared adequately, by contrast, 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 where expertise in conflict management can make a real difference: not only to a company's preparation, but to its response to an emergent attack, and perhaps to its survival.

Too often ignored or short-circuited, preparation here includes a careful analysis of parties with whom a company or nonprofit should consider dealing. And because the real parties, goals and strategies in hybrid warfare are routinely disguised, that analysis is no simple matter. In the future, military and other security agency professionals, who

[26] This is not necessarily a permanent condition. A new article, discusses the possibility that this may change over time, and offers a possible venue. See Honeyman and Tan, above at fn. 2. available at https://drr.scholasticahq.com/article/140835-a-new-management-system-for-a-new-type-of-conflict-singapore-s-possible-role-in-managing-grey-zone-conflict-in-international-commerce

[27] Nancy A. Welsh, Sharon Press and Andrea Kupfer Schneider, Negotiation Theories Engage Hybrid Warfare, 24 Cardozo Journal of Conflict Resolution 543; Chris Honeyman and Ellen Parker, Thinking Ahead in the Grey Zone, 24 Cardozo Journal of Conflict Resolution 617.

[28] Cynthia Alkon and Sanda Kaufman, A Theory of Interests in the Context of Hybrid Warfare: It's Complex. 24 Cardozo Journal of Conflict Resolution 581.

[29] Hinshaw, Borbély and Chrustie above at fn. 25.

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.

It is worth noting that such prospective larger-scale collaborations themselves constitute one area that will clearly call for expertise in conflict management and negotiation. The creation and maintenance of the military / security / civil partnerships called for here will not be simple: in a common English phrase, these groups are "chalk and cheese", with at best limited experience and facilities for dealing productively with each other. Fortunately, getting dissimilar groups of people to work productively together toward their common good is at the very core of several kinds of negotiation expertise – among which public policy mediation is just the most obvious, and in which the last few decades have developed a corps of known-expert practitioners. Such partnerships will call for talent, consistent effort, and of course funding. But the conflict management field can at least offer one great strength: people who already know how to create effective collaborations between very different people.[30]

Many, many more challenges will undoubtedly appear, and as participants in our group have often remarked, if we don't apply an attitude of humility, our subject is one which will teach it to us. We know that this book is coming out while our collective reflections are still in their infancy. A more enduring academic-practitioner community still needs to be structured around such issues. We hope this book will form part of the impetus for it.

In the near term, companies, hospitals, nonprofits, think-tanks, municipalities and most other targets will continue to lack the resources of national governments in trying to ward off and resolve hybrid warfare attacks. But at least a start is now being made toward providing the foundational materials and courses.[31] These are intended to assist in orienting and preparing professionals in many organizations to become more effective at defending their organizations.

All the contributors to these pages hope that this book will help.

Note: From Project Seshat to the Council on Countering Hybrid Warfare

This book is the culminating product of Project Seshat. The project started in early 2020 (after six months' preparatory work) and immediately had to contend with the covid pandemic's restrictions. Its members met physically twice, in Canada in July 2022 and in Belgium in June 2023. The latter meeting was the first occasion for project members

[30] There are even examples of still more creative and perhaps rather startling combinations that have proved productive, e.g. one of uniformed professionals—in this case, police—working with an artist, two psychologists, a conflict management specialist, a sociologist, five poets and an emergency-room physician to design and enact a course for training rank-and-file officers in at least the basic skills of a hostage negotiator (see Rachel Parish and Jack J. Cambria, *The Other Side of The Door: The Art of Compassion In Policing*, DRI Press, 2020.)

[31] The first known for-credit course on the impact of hybrid warfare on law and lawyers' practice was taught in the fall of 2024, by Professor Cynthia Alkon, who heads the criminal law program at Texas A&M Law School.

to meet and exchange ideas with representatives of NATO and of diplomatic think-tanks interested in security issues.

Project Seshat, like its conflict management predecessor projects,[32] was designed to be nimble, adaptable, and open to including a wide variety of people, with a shared entrepreneurial spirit and sense of purpose. The main outcome of the project is, we believe, the first sustained academic effort at publishing on hybrid warfare beyond the realm of military or other security personnel. Prior to this book, Project Seshat produced, among other things, a special issue of the Canadian Defense Association Institute's journal *On Track* and a special issue of the *Cardozo Journal of Conflict Resolution* (both amply cited in this chapter). We would like to take this opportunity to thank everyone involved.

Some original members of Project Seshat have since worked to develop a more sustainable structure. In 2024, they founded the Council on Countering Hybrid Warfare (CCHW), and they are working toward institutionalizing it as a research initiative attached to the Cardozo Law School at Yeshiva University (New York City).

CCHW's explicit mission is to enhance the capacity and respond to the threat of hybrid warfare through a conflict management framework, inclusive of civil society and military cooperation. The Council assisted in formulating and presenting the program of the 2024 Vancouver International Security Summit[33] and is preparing several academic and professional events for the years to come.

Publication of this book marks the formal close of Project Seshat, and future related action along these lines will be by the Council on Countering Hybrid Warfare.

[32] See e.g. the Canon of Negotiation Initiative (2003–present) (discussed at https://www.convenor.com/canon-of-negotiation.html) and the Rethinking Negotiation Teaching project (2007–2013) (discussed at https://www.convenor.com/rethinking-negotiation-teaching.html). Together these projects have involved scholars and practitioners from more than forty fields and have produced over 350 published articles and book chapters.

[33] https://www.rebootcommunications.com/event/viss2024