LAW, CONFLICT, AND HYBRID WARFARE: A TEACHING IMPERATIVE FOR A CHANGING WORLD

Cynthia Alkon* and Andrea Kupfer Schneider**

ABSTRACT

Lawyers increasingly find themselves at the frontlines of the battlefield, just not in the traditional sense. Hybrid warfare is a conflict form that combines traditional military offensive measures with nontraditional methods, including the harnessing of legal systems to achieve strategic goals. Lawyers have always been at the frontline of typical legal risk assessment, thinking about a client's risk of liability or regulation costs generally. Now, lawyers must stand at the ready for a lot more: lawyers must be prepared for cyber-attacks, disinformation campaigns using artificial intelligence, the use of court systems to suppress reporting or shield bad actors, and so much more. Gone are the days where traditional lawyering is the sole line of support that lawyers can offer. A lawyer's negotiation and mediation skills must be honed and trained in hybrid warfare to be an asset to clients experiencing these events. This Essay explains what hybrid warfare is, its evolution, and how it is going to appear before public and private sector lawyers across the globe. It will cover the goals and missions of the first course seeking to train lawyers in hybrid warfare. As the world changes, as methods of combat evolve, and as client needs change accordingly, lawyers must do the same.

INTRODUCTION

Hybrid warfare is a form of conflict that combines conventional military force with nontraditional methods—including cyberattacks, economic pressure, disinformation, and the manipulation of legal systems (lawfare)—

* Professor of Law, Director of the Criminal Law, Justice, & Policy Program, Texas A&M University School of Law; Senior Fellow & Steering Committee Member, Council on Countering Hybrid Warfare.

** Professor of Law, Director of the Kukin Program for Conflict Resolution, Cardozo School of Law, Yeshiva University; Executive Director of the Council on Countering Hybrid Warfare.

to achieve strategic goals. These threats often exploit vulnerabilities in democratic institutions and infrastructures. However, unlike other forms of warfare, lawyers are often in the frontlines and can be among the first to respond to the immediate attack as well as managing the myriad governmental regulations, business decisions, mitigation, and recovery.

While lawyers have always been at the forefront of legal risk analysis through typical risk assessment—of potential litigation or regulation costs—this crossroads of national security, foreign threat, and globalized avenues is a new area of concern. How should lawyers be prepared to help their clients in this new arena? Conflict resolution skills and analysis can support companies and their lawyers in preparing for crisis management and in responding to these now inevitable disruptions when they occur. These tools can also help lawyers recognize when their clients are in a hybrid warfare situation and the different responses that might be appropriate as compared to a conventional legal conflict.

This Essay will initially explain the field of hybrid warfare and how it has evolved as a primary challenge for the next generation of public and private sector lawyers around the world. Second, the Essay will outline the first course taught on hybrid warfare and conflict management, discussing its pedagogy and lessons from the course.

I. WHAT IS HYBRID WARFARE?

Hybrid warfare and gray zone conflict are two relatively new terms that describe a growing category of hostilities in international relations—those that fall between conventional war and outright peace.[1] While the terminology may be new, the core concept is not: rival states have long sought to undermine each other through indirect means—disrupting economies, sowing internal discord, eroding legitimacy, and

1. The term 'hybrid warfare' was first used in the late 1990s, but it gained significant attention in 2005 when Lieutenant General James N. Mattis and retired Lieutenant Colonel Frank Hoffman discussed it in a paper. John G.L.J. Jacobs & Martijn W.M. Kitzen, *Hybrid Warfare*, OXFORD BIBLIOGRAPHIES (Sep. 22, 2021), https://www.oxfordbibliographies.com/display/document/obo-9780199743292/obo-9780199743292-0260.xml [https://perma.cc/RRR6-6K76]. Similarly, 'gray zone' warfare is new. Philip Kapusta coined the phrase in 2015 within a white paper. *See generally* PHILIP PAKUSTA, THE GRAY ZONE (2015), https://specialforcestraining.info/docs/GrayZones-USSOCOM-WhitePaper9Sep2015.pdf [https://perma.cc/BT27-SBJM].

weakening alliances.

Yet these 'typical' conflicts are increasingly characterized by ambiguity: the perpetrators may not appear to be state actors, the tools are often non-military, and the targets frequently lie within the private and nonprofit sectors; including public institutions, NGOs, businesses, or infrastructure—which may or may not have any military component at all.[2]

What distinguishes these actions from earlier disruptions funded by competing governments is their breadth, their ostensible deniability by the attackers or the targets, and the coordination they often exhibit across state, private, and nonprofit actors from hostile or illiberal states seeking to attack democracies. Standard methods include cyberattacks, financial subversion, disinformation campaigns, corruption, espionage, and even the manipulation of legal systems. Each of these elements are explained further below.

A. Multi-Domain and Non-Kinetic Focus

Hybrid warfare often integrates a wide array of tools and instruments instead of relying solely on military elements or kinetic (violent) force.[3] In the last decade, this daunting list includes:

- Cyber tools and cyberattacks, such as ransomware, aimed at disrupting public and private infrastructure systems,[4] extorting money from the targets (by holding medical data hostage, for example), or collecting intelligence about users or customers of the business (like the well-known SolarWinds attack).[5]

2. Chris Honeyman & Andrea Kupfer Schneider, *Introduction: Negotiation Strategies for War by Other Means*, 24 CARDOZO J. CONFLICT RESOL. 487, 488 (2023); Christopher A. Corpora, *How to Undermine a Nation-State in 120 Days: Mediation and Negotiation in a Hybrid Warfare World*, 24 CARDOZO J. CONFLICT RESOL. 503, 505 (2023); Nancy A. Welsh, Sharon Press & Andrea Kupfer Schneider, *Negotiation Theories Engage Hybrid Warfare*, 24 CARDOZO J. CONFLICT RESOL. 543, 543 (2023). Steven Desjardins, *Hybrid Warfare – Is it New, is it Real, and What are the Threats, Vulnerabilities, and Implications for Defence and the Military?*, ON TRACK, Feb. 2023, at 37.

3. Desjardins, *supra* note 2, at 38.

4. Rachana Pradhan & Kate Wells, *Cyberattack Led to Harrowing Lapses at Ascension Hospitals, Clinicians Say*, NPR (June 19, 2024, 5:00 AM), https://www.npr.org/2024/06/19/nx-s1-5010219/ascension-hospital-ransomware-attack-care-lapses [https://perma.cc/VR7Y-82KR].

5. Deven R. Desai & Christos A. Makridis, *Identifying Critical Infrastructure in a World with*

Cyberattacks can also target the "internet of things" from critical infrastructure[6] to voting machines to work-at-home software to fish tanks![7]

- Disinformation campaigns,[8] including fake news, deep-fakes,[9] internet "trolling" of particular targets, and propaganda, used to influence elections, spread misinformation, and polarize societies.[10] Amplifying polarizing messages on social media or using social media to question the legitimacy of democratic elections stems back to at least the 2016 election in the United States (U.S.) and is a model used by Russia in

Supply Chain and Cross-Sectoral Cybersecurity Risk, 62 JURIMETRICS 173, 177–81 (2022) (describing the Solar Winds, Colonial Pipeline, and other hacking attacks designed to threaten key infrastructure); Art Hinshaw, Adrian Borbely & Calvin Chrustie, *Where Is Negotiation in Hybrid Warfare?*, 24 CARDOZO J. CONFLICT RESOL. 517, 532 (2023) (examining ways to reimagine negotiation in the context of cyberattack scenarios); Cynthia Alkon & Sanda Kaufman, *A Theory of Interests in the Context of Hybrid Warfare: It's Complex*, 24 CARDOZO J. CONFLICT RESOL. 581, 583 (2023).

6. Zack Whittaker, *Norway Spy Chief Blames Russian Hackers for Hijacking Dam*, TECHCRUNCH (Aug. 14, 2025, 11:32 AM), https://techcrunch.com/2025/08/14/norway-spy-chief-blames-russian-hackers-for-hijacking-dam/ [https://perma.cc/46VN-VCZH] (outlining a recent attack on a Norwegian dam by Russian hackers).

7. Desai & Makridis, *supra* note 5, at 177.

8. Kevin Matthe Caramancion et al., *The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats*, DATA, Apr. 2022, at 16 (arguing that disinformation should be added to the list of cyber threats); Leticia Bode, *User Correction as a Tool in the Battle Against Social Media Misinformation,* 4 GEO. L. TECH. REV. 367, 377 (2020) (noting that technological solutions alone cannot solve the problem of misinformation on social media and that other players, such as fact checkers, public health organizations, and tech companies should play a role in defeating misinformation).

9. Nina I. Brown, *Deepfakes and the Weaponization of Disinformation,* 23 VA. J. L. & TECH. 1, 9–11 (2020) (noting that even challenging the authenticity of deepfakes themselves can actually lead to greater societal harm and the erosion of public trust. Moreover, fixing or responding to deepfakes through technological solutions have a low success rate.).

10. Terry L. Thompson, *No Silver Bullet: Fighting Russian Disinformation Requires Multiple Actions*, 21 GEO. J. INT'L AFF. 182, 182 (2020).

> In March 2020, US intelligence officials described Russian efforts to aggravate racial tensions by promoting white supremacist groups in private Facebook groups and anonymous message boards . . . Or, in the words of a senior FBI official, "To put it simply, in this space, Russia wants to watch us tear ourselves apart."

Id.

elections around the world.[11] As one long-time observer put it:

> [T]he Russian effort to sow discord and mistrust is relentless. Inspired by President Vladimir Putin's desire to turn Americans against one another and armed with increasingly sophisticated cyber operators in the Russian military, Russian disinformation has become a powerful twenty-first-century information weapon that will not be easily defeated. Russian tactics are constantly evolving, and rapid advances in artificial intelligence and deep-fake videos will make detecting disinformation and pursuing other active measures increasingly difficult in 2020 and beyond.[12]

- Economic measures, such as long-term loans for infrastructure projects (e.g., China's Belt and Road scheme), cornering markets of critical resources (e.g., rare earths, energy, agriculture), trade boycotts, and pressure on foreign companies to share intellectual property (often by purchasing these companies through shell corporations only to be unleashed later).[13]
- Weaponization of legal systems and lawfare where legal actions (e.g., defamation lawsuits) are instigated to suppress reporting, scare witnesses, or slow economic progress by sowing fear among companies that might otherwise invest.[14] In other cases, hybrid

11. Scott J. Shackelford et al., *Defending Democracy: Taking Stock of the Global Fight Against Digital Repression, Disinformation, and Election Insecurity*, 77 WASH. & LEE L. REV. 1747, 1750 (2020); Corpora, *supra* note 2, at 506–07 (explaining internet "trolling" with the example of Russian internet trolling targeted against US-funded activities to provide civil defense support to civilians in contested spaces of Northwest Syria).

12. Thompson, *supra* note 10, at 184.

13. Corpora, *supra* note 2, at 504 (using China's Belt and Road Scheme as an example to illustrate the use of long-term loans for infrastructure projects to economically "invade" vulnerable countries); Sanda Kaufman, *How Should the Whole-of-Society Respond to Hybrid Warfare?*, ON TRACK, Feb. 2023, at 48.

14. Corpora, *supra* note 2, at 507 (illustrating lawfare with the example of the CCP weaponizing the legal system against Sam Cooper, author of *Wilful Blindness*); Calvin Chrustie, *Mind the Hybrid Warfare Gap*, ON TRACK, Feb. 2023, at 21 (providing an example of lawfare where a Canadian journalist

warfare weaponizes legal systems to attack investigative journalism and academic research. For example, outside (allegedly Chinese) funding of legal action in the Canadian courts against journalist Sam Cooper, author of *Wilful Blindness*,[15] has reportedly been used to discredit his findings and discourage others from pursuing similar investigations that highlight the connections between the Chinese government and certain Canadian politicians.[16]

- Transnational organized crime, including illicit finance, money laundering, ransomware, and kidnappings.[17]
- Subversion and sabotage, including direct and indirect support to insurgent groups or internal resistance movements, and actions aimed at undermining public and market confidence.[18] Nations also use third parties and front organizations to fund and amplify opposition groups in target nations, thereby slowing or derailing private sector activities that pose economic or strategic challenges to the aggressor. This often includes filing lawsuits or launching regulatory complaints to further stall projects.[19]
- "Hostage diplomacy" or kidnappings for political leverage or ransom (consider the detention of

reporting on Chinese hybrid warfare faced multiple defamation suits allegedly funded by associates of the Chinese Communist Party to suppress his reporting).

15. *See generally* SAM COOPER, WILFUL BLINDNESS (2021).

16. *See* Sebastian Rotella, *Talking to an Investigative Reporter Who Exposed Chinese Influence in Canada*, PRO PUBLICA (Jan. 6, 2023), https://www.propublica.org/article/sam-cooper-interview-china-canada-influence [https://perma.cc/G2RW-6737].

17. Welsh, Press & Schneider, *supra* note 2, at 544.

18. Honeyman & Schneider, *supra* note 2, at 488.

19. One area of frequent CCP activity is in the rare earths sector, where disinformation and legal interference have been used to frustrate efforts to develop non-Chinese sources of supply. *See generally* Dong v. Global News (2024), 2024 ONSC 3532 (Can. Ont. Sup. Ct. J.).

basketball star Brittney Griner in Russia for 10 months, finally released in a prisoner exchange).[20]

- Covert acquisition of foreign national infrastructure and assets, often disguised as normal commercial dealings.[21]
- Infiltration of academia and Research & Development (R&D) to gain an edge in emerging technologies.[22]

To summarize, hybrid attacks purposefully target civilian and commercial interests to instigate chaos, create disruptions, and weaken or soften an adversary by threatening the infrastructure or legal structure.[23] The objective is to attain dominance and increase global influence without engaging in conventional combat. The ultimate goal for these illiberal states that engage in hybrid warfare is often their own regime preservation and the extension of their power beyond their borders.[24]

B. Methods of Attack

The defining character of hybrid warfare lies not in a singular act of aggression but in its use of diverse and overlapping methods, sustained over time, that combine several distinct forms. First, technological enablement and complex systems allow adversaries to use advances in cyber and communications tools to magnify risks and expand their reach. Second, ambiguity and deniability are central, as attackers intentionally obscure their identity and motivations, leaving defenders uncertain about whether an incident is state-sponsored, criminal, or accidental. Third, hybrid warfare

20. T.J. Quinn, *Inside Brittney Griner's Russia Arrest, Detainment and Release*, ESPN (Dec. 8, 2023, 6:50 AM), https://www.espn.com/wnba/story/_/id/39041673/inside-arrest-detainment-release-brittney-griner-russia-viktor-bout [https://perma.cc/8GZX-T7EX]; Michael Crowley, *Griner's Sentence Renews Pressure on President Biden,* N.Y. TIMES (Aug. 5, 2022), https://www.nytimes.com/2022/08/05/us/politics/brittney-griner-russia-biden.html [https://perma.cc/5WRW-RXWW]; Alkon & Kaufman, *supra* note 5, at 583–84; Chrustie, *supra* note 14, at 22 (describing the politically motivated hostage taking of two Canadian citizens by China, framed publicly as a diplomatic dispute but functioning as part of hybrid warfare).

21. Desjardins, *supra* note 2, at 40 (providing the example of China's overt and clandestine acquisition of foreign national infrastructure in Asia, Africa, Europe and Canada, and the discreet acquisition of energy, agriculture and mining sectors, particularly in rare earth minerals).

22. *Id.*

23. Corpora, *supra* note 2, at 505.

24. Desjardins, *supra* note 2, at 39.

often has a strategic and long-term nature, with operations designed to unfold over years, using shifting methods to make it difficult for targets to strategize or defend; and to position attackers for future disruption. Finally, these attacks rely on the exploitation of societal gaps and vulnerabilities, taking advantage of weaknesses in legal, political, and economic systems—especially in open democracies.

i. Technological Enablement and Complexity

The rapid advance of cyber and communications technologies has exponentially enabled greater speed, reach, depth, and persistence in delivering effects, amplifying vulnerabilities and empowering hostile actors.[25]

ii. Ambiguity and Deniability

A defining characteristic of hybrid warfare is the intentional obscurity of the attackers, who may or may not appear connected to a national security apparatus.[26] Deception and denial are standard elements of an attack. For example, was the attack state sponsored? Coordinated by a criminal gang? A mere technical glitch? This creates an atmosphere of ambiguity, doubt, and confusion among defenders and targets who cannot even figure out who the adversary is.[27] This is part of what makes hybrid warfare so disorienting. The same tactics—cyberattacks, disinformation, money laundering, and covert economic manipulation—can also arise naturally in the churn of a globalized, interconnected world. This ambiguity is precisely what hybrid warfare relies upon. It exploits legal, political, and informational gray areas, making attribution difficult and, therefore, coordinated responses more challenging.

25. Shackelford et al., *supra* note 11, at 1763; Kaufman, *supra* note 13, at 46.

26. Honeyman & Schneider, *supra* note 2, at 488.

27. Corpora, *supra* note 2, at 506; Alkon & Kaufman, *supra* note 5, at 596–97 (suggesting that the term VUCA, standing for volatility, uncertainty, complexity, and ambiguity is "an apt description for hybrid warfare"); Desjardins, *supra* note 2, at 38.

iii. Strategic and Long-Term Nature

While some attacks are short-term, hybrid warfare is frequently part of a broader, more long-term strategy, sometimes spanning years or decades. Similar to 'sleeper cells,' malware can be implanted and inactivated for years.[28] An example of this is the Chinese cyber-attack, Volt Typhoon, which targeted infrastructure in the United States.[29] Volt Typhoon sought to attack the Port of Houston, although Port officials caught it before it had taken root.[30] Volt Typhoon is considered a "pre-positioning attack," where large amounts of information do not leave any given system, but instead, the hacker is in the system and ready to strike to disrupt operations at a later date.[31] Volt Typhoon targeted critical infrastructure, but "not against the largest, most significant critical infrastructure in the United States . . . [instead] it is against a broad swath of small-and medium-sized companies that are potentially critical in individual supply chains or just capable of causing societal panic in some place around the country."[32] It is likely still unknown exactly where Volt Typhoon embedded itself and where it could cause problems in the future.[33]

Moreover, hybrid warfare actors maintain an advantage by rapidly adapting their tactics to exploit emerging technologies. Once a target identifies and defends against one form of attack—often at significant cost—it tends to prepare for its recurrence rather than anticipate new methods. Hybrid tactics seem to evolve faster than defenses can, leaving the focus on resources frequently targeted in the past instead of emphasizing threat innovation.

iv. Exploitation of Societal Gaps and Vulnerabilities

Hybrid warfare exploits communication and legal gaps between a

28. Alkon & Kaufman, *supra* note 5, at 590.

29. Jonathan Greig & Martin Matishak, *Any Number Given of Volt Typhoon Victims 'Likely an Underestimate,' CISA Says,* THE RECORD (May 7, 2024), https://therecord.media/volt-typhoon-targets-underestimated-cisa-says [https://perma.cc/NMK9-8GBV].

30. Sarah Coble, *Port of Houston Quells Cyber-Attack*, INFOSECURITY MAGAZINE (Sep. 27, 2021), https://www.infosecurity-magazine.com/news/port-of-houston-quells-cyberattack/ [https://perma.cc/RS46-PSHH].

31. Greig & Matishak, *supra* note 29.

32. *Id.*

33. *Id.*

country's various sectors—civilian and military, legal and civil, municipal/provincial, federal government, and corporate.[34] These vulnerabilities arise from factors such as the complexity of intertwined systems, the lack of transparency in globalized economies, and the lack of preparedness of the public, private, and non-profit sectors.[35] Western democracies, with their open societies and legal systems designed to protect individual rights, can be particularly susceptible to exploitation by authoritarian regimes that operate with fewer constraints.

II. TEACHING LAWYERS SKILLS FOR A HYBRID WARFARE ENVIRONMENT

Although often overlooked, lawyers are on the front lines of hybrid warfare.[36] When attackers target companies or file lawsuits, lawyers are usually the first to respond, including advising on crisis management. Increasingly, lawyers guide clients in environments shaped by hybrid threats that implicate national security, international law, corporate governance, compliance, data privacy, and civil rights.

Yet governments and institutions have been slow to adapt.[37] Military, intelligence, and security agencies remain poorly structured to

34. Chrustie, *supra* note 14, at 15; Desjardins, *supra* note 2, at 38.

35. Chrustie, *supra* note 14, at 16; Kaufman, *supra* note 13, at 47–48.

36. The military has recognized, at least within the JAG corps and the military legal schools, that lawyers need a broader national security focus to better serve the military and government agencies that are their clients. Lisa L. Turner, *Developing Client-Ready Practitioners: Learning How to Practice National Security Law at Military Law Schools*, 7 NAT'L SEC. L. & POL'Y 1, 1–2 (2014) (noting that national security also now should include more than state-to-state armed conflict, including cyberattacks). *See also* James E. Baker, *Process, Practice, and Principle: Teaching National Security Law and the Knowledge that Matters Most*, 27 GEO. J. LEGAL ETHICS 163, 163 (2014) (arguing for classes in national security law at "civilian" law schools).

37. *See, e.g.*, Thompson, *supra* note 10, at 182 (noting the lack of U.S. action). In contrast, the European Union (EU) developed an 'Action Plan Against Disinformation' and a 'Code of Practice on Disinformation,' the latter being a self-regulatory measure to encourage Facebook, Google, and Twitter to take responsibility for their platforms' content. The EU has experienced Russian disinformation in social media during elections, most recently in connection with the 2019 European Parliament elections and the 2017 French and German presidential elections. More broadly, the EU and Baltic countries have felt the impact of Russian gaslighting, propaganda, and disinformation for decades, throughout the Soviet period and continuing in the post-Soviet era. Canada has responded as well. *See e.g.*, Yasmin Dawood, *Protecting Elections from Disinformation: A Multifaceted Public-Private Approach to Social Media and Democratic Speech*, 16 OHIO ST. TECH. L.J. 639, 663 (2020) (outlining that the Canadian government has created norm-based initiatives for private companies, such as the Declaration on Election Integrity and the Digital Charter, to combat election misinformation. Major companies such as Facebook, Microsoft, etc. signed on to the initiatives.).

address threats aimed at private companies and citizens.[38] Lawyers, trained primarily to predict liability and counsel on remedies, often limit their assistance to navigating regulatory disclosure and compliance, without addressing broader or preventive strategies.

Hybrid warfare especially challenges negotiation (a core legal skill). In contexts such as cybercrime, illicit finance, espionage, coercive mergers, and hostage diplomacy, traditional dispute resolution falters. When aggressors are hidden, decentralized, or state-affiliated but disavowed, who is the counterpart with whom to negotiate? And is negotiation even possible when the aggressor has no interest in a lasting resolution? The disruption, uncertainty, and inability to strategize are the goals of the attack. The Volt Typhoon attack is an example. China was later determined to be responsible for Volt Typhoon, but there was no announcement of the attack or demand for payment, and no one party or nation was clearly responsible at the time it was launched.

Training lawyers for hybrid warfare requires moving beyond traditional contract, litigation, and deal-making skills. They must integrate risk and conflict management with knowledge across free speech, regulation, cybersecurity, and technology. Just as critically, lawyers need to help forge underdeveloped connections among companies, governments, and national security actors—connections essential for effective hybrid warfare anticipation and response.

In response to the need to have better prepared lawyers, in the fall semester of 2024, one of us developed and taught the first course on conflict management in hybrid warfare taught at a U.S. law school.[39] What follows is an in-depth description of what the course *Conflict Management and Hybrid Warfare* covered, the pedagogical approaches used, and the class goals.

---

38. Chimène I. Keitner & Harry L. Clark, *Cybersecurity and Trade Agreements: The State of the Art*, 10 HARV. BUS. L. REV. 1, 1 (2019) (outlining that the U.S.-Mexico-Canada Trade Agreement (USMCA) was the first operative U.S. free trade agreement to include a chapter devoted to "digital trade" with explicit cybersecurity provisions).

39. *See generally* Cynthia Alkon, Conflict Management and Hybrid Warfare (Fall 2024) (syllabus, Texas A&M University School of Law) (on file with the *Washington University Journal of Law and Policy*).

A. Teaching Objectives

The course was built around several core learning objectives.[40] Students were expected to develop a working understanding of what hybrid warfare is, and how it manifests in legal practice. This included being able to identify hybrid threats, analyze their implications for clients, and understand how they can apply conflict management theories and tools in these scenarios. Particular attention was paid to the attorney-client relationship in crisis situations, where issues of confidentiality, collaboration, and trust can be especially strained. The course also aimed to foster students' abilities to spot ethical dilemmas, distinguish between the legal and extralegal tools available in a hybrid warfare context, and think critically about how to advise clients facing risk in uncertain, multi-party, and cross-sector situations.

Collaborative skill-building was also a central objective. Students were asked to consider not only how to advise their clients, but also how

40. The learning objectives outlined in the syllabus were:

- To understand what hybrid warfare is
- To understand the possible ways that lawyers may confront hybrid warfare
- To be able to identify when facing hybrid warfare scenarios
- To understand the basic theory and skills of conflict management
- To understand the basics of how to apply conflict management in the context of hybrid warfare
- To understand how hybrid warfare may impact the attorney-client relationship
- To be able to identify ethical issues in representing clients in different hybrid warfare contexts
- To be able to distinguish between the different tools, including the applicable law that are available to a lawyer in a hybrid warfare context
- To be able to assess and advise clients about how to manage the basic risks they may face in the context of hybrid warfare, including a broad understanding of what laws might apply
- To improve collaborative skills to better apply conflict management skills both with the party represented and to work with other parties facing joint hybrid warfare threats
- To be able to think critically about when to use various tools, including conflict management and negotiation skills, when representing clients in a hybrid warfare scenario

Id. at 2.

to work constructively across organizational boundaries—whether with regulators, cybersecurity experts, international partners, or allied institutions. The course emphasized the value of negotiation and conflict management as dynamic tools, rather than static procedures, requiring continuous adaptation to evolving threats and environments.

B. Topics Covered

The eleven students who enrolled in the course had varying backgrounds—one previously worked on hybrid warfare attacks in both the military and civilian cyber sector, some had undergraduate degrees in political science, and others had no background in any of the areas covered in the class, including the geo-political environment breeding hybrid warfare. This meant that the class had to quickly bring everyone up to speed on the basics of hybrid warfare, who some of the key hybrid threat actors attacking the United States are, and what are some of the main hybrid threats.

Topics covered over the semester included an introduction to hybrid warfare and conflict management, negotiation strategies tailored to hybrid threat environments, the concept of wicked problems and whole-of-society responses, dispute system design in crisis contexts, lawfare, cybersecurity and cybercrime, multi-party negotiation, and the challenges of disinformation and election interference.[41] Together, these topics laid a foundation—not just for understanding hybrid warfare, but for responding to it with legal and strategic acumen. The course alternated between examining the nature of hybrid warfare and helping

41. The topics as listed in the syllabus were:

- Introduction to Hybrid Warfare & Conflict Management
- Introduction to Negotiation in the Context of Hybrid Warfare
- Wicked Problems and Whole of Society Tactics of Hybrid Warfare
- Dispute System Design and Planning for Crisis
- Lawfare
- Cyber Security and Cyber Crime
- Multi-Party Negotiation
- Misinformation, Disinformation, Malinformation and Election Interference

Id. at 12–13.

students develop the analytical and practical skills lawyers require to effectively advise clients during potential hybrid warfare incidents and how to prepare for such threats.

C. Pedagogical Approaches and Materials Used

To achieve these goals, the course relied on a mix of instructional strategies and materials. Guest speakers played a vital role, bringing real-world insight from a wide range of sectors, including large law firms, multinational corporations, government agencies, cybersecurity firms, and academia. These speakers provided students with a direct window into the complexity of legal practice in the hybrid warfare arena. Every class had a live guest speaker (or panel of speakers) and each week, students viewed pre-recorded interviews as part of the class preparation materials. This combination gave flexible access to a variety of expert perspectives. The guest speakers came from many different countries and professional backgrounds.[42]

42. The guest speakers, both in person and via pre-recorded zoom interviews, with the titles and positions they held in the Fall of 2024 were:

- Calvin Chrustie, Senior Security and Critical Risk Consultant, and Senior Director and Steering Committee Member of the Council on Countering Hybrid Warfare
- Adrian Borbély, Associate Professor of Negotiation at Emlyon Business School, Lyon, France, Senior Fellow & Steering Committee Member of the Council on Countering Hybrid Warfare
- Chris Corpora, Domain Expert with Hala Systems and Board Member of the International Coalition Against Illicit Economies
- Paula deWitte, Professor of Computer Science & Engineering, Texas A&M University
- Sanda Kaufman, Professor Emerita of Planning, Public Policy and Conflict Management, Cleveland State University
- Chris Honeyman, Managing Partner of Convenor Conflict Management
- Gary Duane Brown, Associate Professor of Practice, The Bush School of Government and Public Service, Texas A&M University
- Anne Leslie, Cloud Risk & Controls Leader EMEA, IMB Cloud for Financial Services
- Andrea Kupfer Schneider, Professor of Law, Director of the Kukin Program for Conflict Resolution at Cardozo School of Law, Executive Director & Steering Committee Member, The Council on Countering Hybrid Warfare

Rather than using traditional simulations, the course featured structured case scenarios that required students to collaborate in groups to problem-solve and advise hypothetical clients. The scenarios were adapted from two scenarios in the book *Hybrid Warfare: A Collection of Scenarios*.[43] These scenarios were designed to mirror the uncertainty and information asymmetry characteristic of hybrid conflicts. Readings from law, national security, and conflict resolution fields were assigned to help students build an interdisciplinary framework for analysis.

The class was offered online. This was done for several reasons. First, being online made it easier for students to directly connect with the guest speakers in each class. All students were required to keep their cameras on and were instructed that part of their class participation grade would be based on active engagement with the speakers. This format also made it easy to have students participate in group work during class through breakout rooms. The class was small, and all the students knew each other and the professor from other classes. For these reasons, the course was able to lessen online education's typical downside of students struggling to make connections with peers and the instructor.

- Janice Fischer, Senior Director & Steering Committee Member, The Council on Countering Hybrid Warfare
- Theodore Kubus, Partner with the law firm Baker Hostetler
- Scott McGregor, Principle of Closehold Intelligence Inc.
- Elizabeth Spencer Berthaiume, Attorney at Law, specialist in Privacy Law
- Greg Dzsinich, Attorney, Board Member of the Cybersecurity Advisors Network (CyAN)
- Leigha Simonton, U.S. Attorney for the Northern District of Texas
- Errin Martin, Assistant U.S. Attorney, Section Chief National Security/Cyber/Money Laundering, Northern District of Texas
- Jongwoo "Daniel" Chung, Assistant U.S. Attorney
- Michelle Winters, Assistant U.S. Attorney
- Dr. Chris Bronk, Assistant Professor, Department of Information and Logistics Technology, College of Technology, University of Houston
- Chris Wolski, former Information Security Officer (ISO-Director) Port of Houston, Adjunct Professor Texas A&M University School of Law

43. *See generally* HYBRID WARFARE: A COLLECTION OF SCENARIOS (Adrian Borbely ed. forthcoming 2026).

D. Assessments

Due to the unique subjects covered, this class did not lend itself to traditional forms of assessment such as exams or quizzes. Instead, students were asked to complete reflective writing assignments. This included discussion questions about the recorded guest speakers and guided assessments of the scenarios, or case studies. The guided assessments included specific questions that intended to hone their analytical skills in identifying a hybrid warfare situation and the conflict management skills and approaches that could be used in such a scenario.

The final assignment was to complete a written, guided analysis of a real-life hybrid warfare scenario, the attempted 2022 Volt Typhon attack on the Port of Houston.[44] Students were assigned readings on the attack, including one identifying it as a Chinese attack and the Port of Houston as

44. Sections from the final written assignment (including the guided questions) are below:

> You are a lawyer working for a large law firm who is representing the Port of Houston as outside counsel, retained by the Head of Cybersecurity. For the purposes of this exercise, you should assume that you have been given the case at the stage when the attempted incursion was discovered. The Head of Cybersecurity has brought this problem to your attention. The senior partner has asked you to write a memo, so she has all the background she needs to proceed forward with the representation. . . . The senior partner has specific questions that she wants answered in this memo:
>
> 1. Describe what happened.
> 2. What laws do you need to be aware of? What is the Port of Houston obligated to do under the law?
> 3. Is this likely hybrid warfare? Explain what facts support your answer.
> 4. What are the Port of Houston's interests at this stage?
> 5. What are the possible points of conflict both in terms of issues and players within the Port of Houston that you might want to prepare for before doing any counseling or facilitating meetings surrounding this incident?
> 6. What experts do you recommend the firm consult about this case? Which ones are employed within the Port and which ones might you need to hire or bring in as outside experts?
> 7. Who are the stakeholders?
> 8. What did the Port of Houston do right in this situation? What are the lessons for the future?
> 9. What do you think you don't know? Does it matter to your analysis or answers to the questions above?

just one of the targets.[45] Chris Wolski, who had been the head of cyber security for the Port of Houston at the time, did a one hour "client interview" via Zoom during which students could ask any questions—giving them a better understanding of the attack and what they, as lawyers, needed to be aware of before advising the Port of Houston about its response. This awareness included both conflict management within the Port of Houston and the regulatory and reporting requirements. Students were free to handle the client interview any way they wanted, and they chose to prepare the questions they wanted to ask in advance, designating one of their classmates to ask the primary questions. The result was a highly polished mock client interview.

E. Underlying Themes—Humility, Awareness, and Conflict Management

There were three underlying themes in the course: humility, awareness, and conflict management. Hybrid warfare is ever changing and, as the examples earlier in this essay demonstrate, daunting in its breadth and scope. Its threat actors, tactics, and targets constantly change. As a result, it is impossible to fully prepare lawyers for every possible scenario. Unlike some areas of law where we expect lawyers

45. Greig & Matishak, *supra* note 29; Coble, *supra* note 30. The assigned reading on the attack included: Sean Lyngaas, *Hackers Breached Computer Network at Key US Port but Did Not Disrupt Operations*, CNN (Sept. 23, 2021, 6:35 PM), https://www.cnn.com/2021/09/23/politics/suspected-foreign-hack-houston/index.html [https://perma.cc/DQ4H-FGVW]; U.S. DEP'T OF JUST., U.S. GOVERNMENT DISRUPTS BOTNET PEOPLE'S REPUBLIC OF CHINA USED TO CONCEAL HACKING OF CRITICAL INFRASTRUCTURE (2024), https://www.justice.gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical [https://perma.cc/RBK2-8UCX]; *Portman Questions Cybersecurity Officials in Wake of ManageEngine Vulnerability and Increased Cyber Attacks*, U.S. SENATE COMM. ON HOMELAND SEC. & GOVTL. AFFS. (Sept. 23, 2021), https://www.hsgac.senate.gov/media/reps/portman-questions-cybersecurity-officials-in-wake-of-manageengine-vulnerability-and-increased-cyberattacks/ [https://perma.cc/5BU7-A2KF]; *APT Actors Exploiting Newly Identified Vulnerability in ManageEngine ADSelfService Plus,* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Nov. 22, 2021), https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-259a [https://perma.cc/F3U8-A372]; *Cybersecurity Policy*, PORT OF HOU. AUTH. (Apr. 2018), https://porthouston.com/wp-content/uploads/2022/11/Cyber_Security_Policy-201804-final.pdf [https://perma.cc/TE2G-FMUB]. Students were also directed to the applicable law regulating the maritime industry: *Coast Guard Maritime Industry Cybersecurity Resource Center*, U.S. COAST GUARD, https://www.uscg.mil/MaritimeCyber/ [https://perma.cc/AJG7-2L5U]; Sean Lyngaas, *Biden Administration to Issue New Cyber Directives Aimed at Defending Ports, Invest Billions in New Port Infrastructure*, CNN (Feb. 21, 2024, 7:39 PM), https://www.cnn.com/2024/02/21/politics/biden-new-cyber-directives-maritime-ports [https://perma.cc/5UVU-2ZNK] (detailing changes to the law in 2024).

to 'know it all' or nearly all, that is not a realistic expectation in hybrid warfare. In fact, thinking that we 'know it all' could be dangerous and lead to serious mistakes. Therefore, the first underlying theme of the course was humility. Multiple guest speakers talked about the need to be humble, to recognize that there is much you do not know, and likely cannot know, in a hybrid warfare situation. Hybrid warfare demands that lawyers listen more, ask more questions, and look to other disciplines and experience. Being humble in recognizing these inherent uncertainties was a core and recurring theme.

Another core theme was hybrid warfare awareness. Because so few lawyers have any background in hybrid warfare, they often confuse a hybrid attack with something more conventional. A cyberattack with a ransom demand could be a simple cybercrime, but it could also be a hybrid warfare attack. Understanding whether the incident is a hybrid warfare attack could change the approach or the advice given to a client significantly. Lawyers should consider that option and, even if they may never definitively know the answer, should be aware of what might be different if the attack is hybrid warfare.

The final theme of the class was linking conflict management skills to the lawyer's new portfolio of potential responsibilities. In every class, students read about or discussed conflict management skills—what they are in different contexts, why they matter, and how to improve them. What does this mean in practice? In the case of the Volt Typhoon attack on the Port of Houston, recognizing that the Chinese government was behind the attack changed some core elements of the response. The Port of Houston was required, regardless of the origin of the attack, to report the attack to the U.S. Coast Guard (as the regulatory authority over ports). But once the attack was identified as the Chinese government trying to embed a virus to lay dormant in the Port's computer system, the Port had to take security measures assuming there might be a future attack, given an attacker with tremendous resources. This was not an attack from a cyber-crime group randomly hitting different targets to see what might stick.

Once lawyers are aware that hybrid warfare is an option, it demands that they not jump to conclusions quickly (going back to humility) and that they advise their clients about both short-term responses and long-term protection while being mindful that the attackers may have both

deeper pockets and a long-term view that extends beyond that of the client—this also means clients may be targeted again and again. Lawyers who can bring conflict management tools to anticipate and respond more effectively will serve their clients well in this new threat environment.

CONCLUSION

Hybrid warfare is no longer an abstract or peripheral concern—it is a defining feature of the contemporary security landscape. It reaches hospitals, law firms, corporations, universities, and government institutions. The examples mentioned in this essay—from ransomware attacks on public infrastructure to state-sponsored lawfare—suggest that these tactics are ongoing, escalating, and increasingly sophisticated. They aim to exploit the seams between public and private sectors, the gaps in regulatory frameworks, and the vulnerabilities inherent in democracies.

In this environment, lawyers play an indispensable role. They are often the first professionals called upon to respond, interpret, and advise in the midst of uncertainty. Yet their traditional training does not sufficiently prepare them for the challenges of hybrid conflict. Advising a client in the wake of a ransomware attack, a disinformation campaign, or a covert acquisition attempt requires skills that blend legal analysis with risk management and conflict management skills. Lawyers must be able to recognize when a seemingly routine dispute or regulatory challenge is part of a broader scheme of hybrid warfare.

The imperative, then, is pedagogical as much as professional. As the course described demonstrates, interdisciplinary teaching—drawing on law, conflict resolution, security studies, and technology—can give students both conceptual frameworks and practical skills. Just as important, it can cultivate humility and awareness: the recognition that no lawyer will ever 'know it all' in hybrid warfare, but that lawyers can and must learn to ask the correct questions, build the right partnerships with government and national security institutions, and advise their clients accordingly.

Ultimately, hybrid warfare erodes the very systems of trust and order upon which law depends. Training lawyers to respond effectively to hybrid threats is essential to preserve democratic institutions, safeguarding fundamental rights, and enable societies to withstand disruption. The teaching imperative is inseparable from the professional one: preparing

lawyers to serve as frontline responders in hybrid conflicts is a necessary step toward resilience in a rapidly changing world.