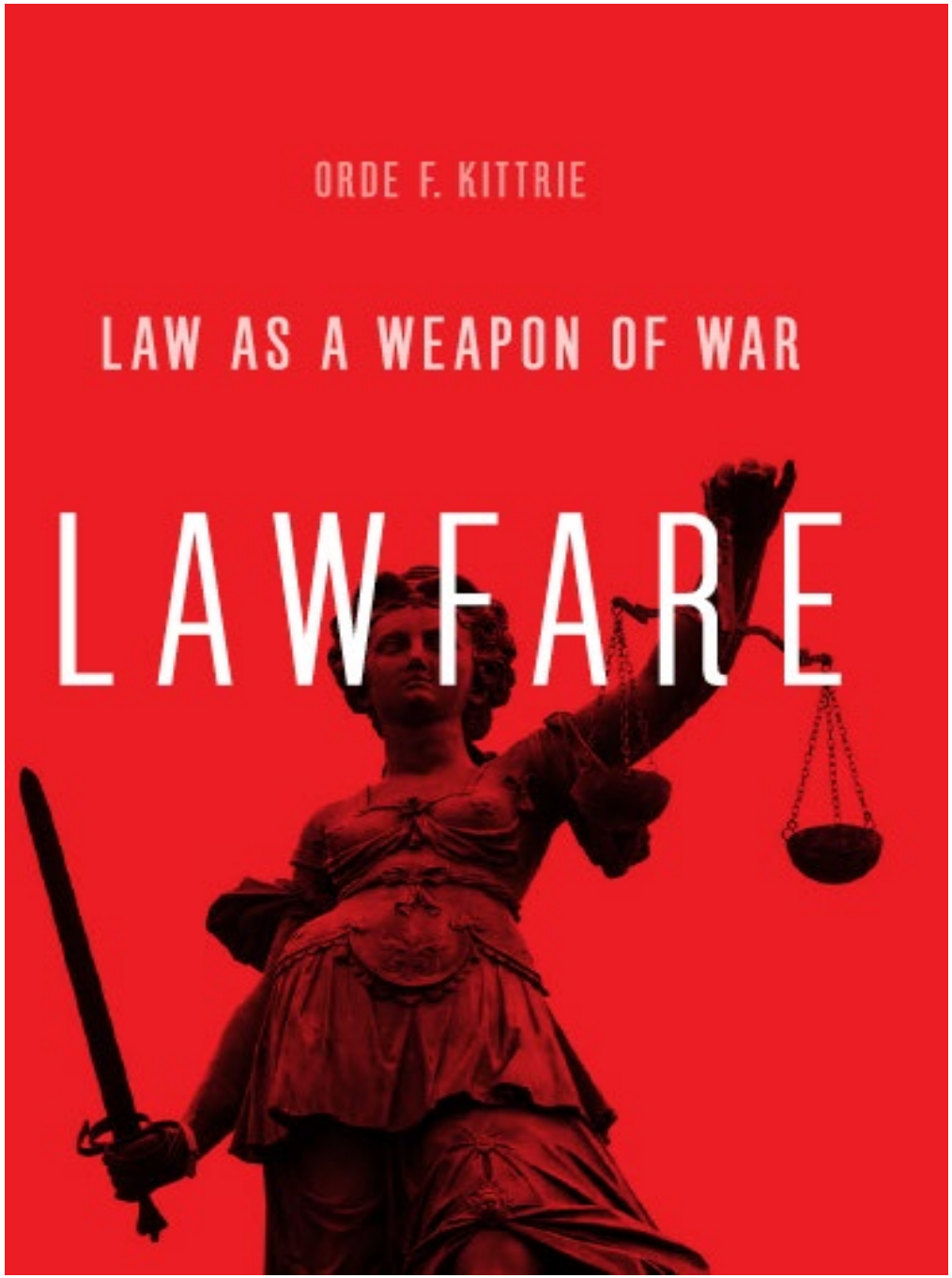
ORDE F. KITTRIE
LAW AS A WEAPON OF WAR
LAWFARE

“Lawfare” is:

-- the strategy of “using – or misusing – law as a substitute for traditional military means to achieve a warfighting objective”

-- “simply another kind of weapon, one that is produced, metaphorically speaking, by beating law books into swords.”

-- Major General Charles Dunlap (ret.), former USAF Deputy JAG

"Law has evolved to become a decisive element – and sometimes *the* decisive element – of contemporary conflicts."

-- Major General Charles Dunlap, Jr. (ret.), former Deputy Judge Advocate General of the U.S. Air Force

Who is Waging Lawfare:

- U.S. governments (federal, state, local)
- Alliances and allied/partner governments (e.g., NATO, UK, Israel)
- Adversary governments (e.g., China)
- Militant organizations (e.g., Islamic State, Hamas, Hizballah, Taliban)
- Non-violent NGOs (e.g., Shurat Hadin, Hind Rajab)
- Private sector attorneys

What makes lawfare an increasingly powerful tool in 21st century conflicts?

1) The increased number and reach of international laws and tribunals

2) The rise of NGOs focused on law of armed conflict and related issues

3) The information technology revolution

4) Globalization and economic interdependence

NATO and Lawfare ("Legal Operations")

- NATO Supreme Headquarters Allied Powers Europe issued a legal operations directive and created a centralized "Legal Operations Team"
- NATO/SHAPE directive defines "legal operations" as "the use of law as an instrument of power," including any actions in the international "legal environment by state or non-state actors aimed at, among others, gaining/undermining legitimacy, advancing/undermining interests, or enhancing/denying capabilities, whether at the tactical, operational and/or strategic/political levels."

Lawfare by People's Republic of China

- 1996: PRC President Jiang Zemin announces China "must be adept at using international law as a weapon"
- 2003: PRC Communist Party Central Committee and PRC Central Military Commission adopt "legal warfare" as major component of China's strategic doctrine
- Today, PRC systematically waging lawfare against U.S. and its allies in maritime, information technology, aviation, cyber, space, nonpro, Taiwan, and other arenas

“Defeating the enemy without fighting is the pinnacle of excellence.”

-- Sun Tzu

“War has rules, but those rules are set by the West . . . so do we need to fight according to your rules? No.”

-- Wang Xiangsui, co-author of the influential book *Unrestricted Warfare*

"We should therefore always apply international laws flexibly . . . appealing to those aspects beneficial to our country while evading those detrimental to our interests." – PRC military's BASICS OF INTERNATIONAL LAW FOR MODERN SOLDIERS

"Every soldier, sailor, airman, marine . . . must comply with the LOAC [and JAGs] must advise commanders and U.S. forces to follow its requirements exactly." – U.S. Army's OPERATIONAL LAW HANDBOOK

Western vs. China Lawfare in the Information Technology Domain

The Stakes:

--$500 billion per year in intellectual property theft from just the U.S.

-- Ability to hyper-personalize brink & conduct of kinetic conflict by direct outreach to warfighters & their families, using stolen financial, health, genetic, other personal data

-- Ability to shut down critical electrical and other infrastructure without firing a shot

Western vs. China Lawfare in the Information Technology Domain

PRC Use of Laws as Weapons:

--Require partnerships with Chinese firms

-- Require data storage in China

-- PRC access to & control of data in China

-- Require Chinese firms cooperate w/ PRC intel

-- Banning Western social media, messaging apps

-- Attempting to dominate int'l standards setting organizations

Western vs. China Lawfare in the Information Technology Domain

US Use of Laws as Weapons:

--Restrict the use of Tik Tok on US govt devices

-- Ban Tik Tok in US unless Bytedance divests

-- Move to ban PRC drones in US

-- Prosecute PRC hackers

-- Committee on Foreign Investment in the U.S.

-- Prohibit US govt use of Huawei equipment&services

-- Prohibit Huawei & ZTE equipment sales in US

-- Limit Huawei access to foreign-produced semiconductors made with US technologies

-- Charged Huawei with fraud, sanctions violations, etc.

Sweden, Germany, Estonia, Romania banned Huawei from their 5G networks

The Lawfare Battle over Huawei's Capacity to Shut Western Critical Infrastructure

Australia banned Huawei products from its 5G network in 2018, after the director-general of Australian government's Signals Directorate determined that Huawei products would risk PRC "interception of telephone calls" and much of Australia's critical infrastructure would come to be dependent on 5G and Beijing would be able to order Huawei to shut it off. PRC law requires all Chinese persons and companies to co-operate with the government on any national security matter.

BBC

How oil has brought Russia, China and India closer

2 September 2025

Share Save

Osmond Chia

Business reporter, BBC News, Singapore

Russian Oil Prices Sink as India and China Cut Purchases Ahead of U.S. Sanctions Deadline

“U.S. microchips continue to guide and power the Russian weapons that kill Ukrainians daily. . . as U.S. semiconductor export controls have continued to fail.”

“The Subcommittee’s investigation found that U.S. semiconductor manufacturer efforts have been abjectly lacking.”

-- US Senate Subcommittee report, December 24, 2024

THE U.S. TECHNOLOGY FUELING RUSSIA'S WAR IN UKRAINE:

EXAMINING THE BUREAU OF INDUSTRY AND SECURITY'S ENFORCEMENT OF SEMICONDUCTOR EXPORT CONTROLS

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

"The Subcommittee's inquiry has revealed that enforcement of export controls is a shadow of what it should be, and inadequate at every level. BIS is asked to fulfill a key national security function on a shoestring budget, forcing it to trace increasingly sophisticated distribution networks while relying on laughable technology that has not been meaningfully updated for nearly two decades. But, even with these constraints, BIS's enforcement efforts have been inadequate."

"BIS has not charged companies with sufficiently serious violations or imposed fines sufficiently robust to compel better compliance."